Branching bisimulation for context-free processes

Didier Caucal, Dung Huynh, Lu Tian

Rapports de Recherche

1992

25ème anniversaire

N° 1789

Programme 2
Calcul Symbolique, Programmation et Génie logiciel

BRANCHING BISIMULATION FOR CONTEXT-FREE PROCESSES

Didier CAUCAL
Dung HUYNH
Lu TIAN

Novembre 1992

IRISA

INSTITUT DE RECHERCHE EN INFORMATIQUE
ET SYSTEMES ALEATOIRES

Campus Universitaire de Beaulieu
35042 - RENNES CEDEX FRANCE
Tél. : 99 84 71 00 - Télex : UNIRISA 950 473 F
Télécopie : 99 38 38 32

Branching Bisimulation for Context-free Processes

Didier CAUCAL
IRISA
Campus de Beaulieu
35042 Rennes, France
E-mail: caucal@irisa.fr

Dung HUYNH Lu TIAN
University of Texas at Dallas
Computer Science Program
Richardson, TX 75083, USA
huynh@utdallas.edu, ltian@utdallas.edu

Projet MICAS
Programme 2
Publication Interne n° 680 - Octobre 1992 - 36 pages

Abstract The branching bisimulation defined by Van Glabbeek and Weijland takes care of preserving the branching structure of processes even though silent actions are taken. Branching bisimulation is obviously decidable for finite state processes. A proof that it is also decidable for reduced and proper context-free processes has been given by Hüttel. Going further along these lines, we prove that the class of reduced and proper context-free processes is closed under quotient by their greatest branching bisimulation. Moreover, the construction of the factor graph is in PSPACE.

Bisimulation de branchement de Processus Algébriques

Résumé La bisimulation de branchement définie par Van Glabbeek et Weijland préserve la structure de branchement des processus avec actions silencieuses. La bisimulation de branchement est trivialement décidable pour les processus d'états finis. Hüttel a montré que la bisimulation de branchement reste décidable pour des processus algébriques réduits et propres. Allant plus loin dans cette direction, on montre que la classe des processus algébriques réduits et propres est fermée par quotient selon la plus grande bisimulation de branchement. De plus, la construction du graphe quotient est en PSPACE.

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE (U.R.A. 227) UNIVERSITE DE RENNES I I.N.S.A. DE RENNES
INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE (UNITE DE RECHERCHE DE RENNES)

BRANCHING BISIMULATION FOR CONTEXT-FREE PROCESSES *

Didier CAUCAL
IRISA
Campus de Beaulieu
35042 Rennes, France
E-mail: caucal@irisa.fr

Dung HUYNH
University of Texas at Dallas
Computer Science Program
Richardson, TX 75083, USA
huynh@utdallas.edu, ltian@utdallas.edu

Lu TIAN

1 Introduction

We will study branching bisimulation for a restricted class of SOS definable processes, including not only the finite state processes usually considered for verification purpose, but also the context-free processes, that is the recursively defined BPA processes of Bergstra and Klop [BK 88]. For those context-free processes, we are not only concerned with the decision of branching bisimulation, but also with the effective construction of factor processes. We will show that whenever branching bisimulation is decidable for a subclass of context-free processes, the associated factor processes are context-free. This is not evident since factoring a class by an effective equivalence leads in general outside that class.

Context-free processes are exactly those labeled transition systems which are induced by alphabetic string-rewrite systems constrained to prefix rewriting. Those transition systems are specified in the SOS style [GV 89] by a finite set of axioms $u \xrightarrow{a} v$ whose left members u are letters and right members v are strings, plus one contextual rule, the rule of prefix rewriting:

$$\frac{u \xrightarrow{a} v}{uw \xrightarrow{a} vw} \quad .$$

Each finite string induces a *context-free process*, defined as the transition graph originated from that string. The context-free processes are [Ca 90 b] rooted equational graphs of finite degree, and therefrom, it follows that properties of cf-processes expressed in monadic second-order logic are decidable [Co 90]. Nevertheless, this does not extend to bisimulation properties, and direct proofs must be given in order to show their decidability. A direct proof of the decision of strong bisimulation for reduced cf-processes was given in [BBK 87], [Ca 90 a], [HS 91], and a Σ_2^p upper bound has been obtained in [HT 92]. An extended proof was proposed for branching bisimulation in [Hü 91].

*Without the complexity section, this article will be presented at FSTTCS 92 and will appear in LNCS. The complexity section will be presented at the Allerton conference.

It is one thing to establish the decision of an equivalence, it is another thing to give an effective construction for the factor models. We will address the second issue, which is of a certain importance for optimizing process verification techniques. Since we have already solved that problem for strong bisimulation of (reduced) cf-processes in [Ca 90 a], we will consider only branching bisimulation in the sequel. By the way, we will also prove that cf-processes are effectively closed under quotient by branching bisimulation.

The remaining sections are organized as follows. In Section 2, we characterize the quotient of a graph by its greatest branching bisimulation as the canonical reduct of that graph for an adequate notion of graph reduction. We then focus in Section 3 on (reduced and proper) context-free processes and show in that restricted framework, the quotient operation is effective and produces (reduced and proper) context-free processes. Finally in Section 4, we show that the decision of branching bisimulation for cf-processes is in the second level Σ_2^p of the polynomial time hierarchy [St 77], instead of an at least exponential space complexity of the algorithm in [Hü 91]. Furthermore, we show that minimization of context-free processes is also in polynomial space.
All the proofs are given in the appendix.

2 Branching bisimulation and canonical reducts

In this section, we recall the definition of branching bisimulation and characterize the quotient of a graph by its greatest branching bisimulation as a maximal graph reduction (Theorem 2.9). Here, a *graph* is an infinite set of *arcs* (p, a, q) with source p, goal q, and label $a \in T \cup \{\epsilon\}$, where T is an *alphabet* and ϵ is the empty word. Every arc (p, a, q) may be identified with a *labeled transition* $p \xrightarrow{a} q$. The one step transition relations $\xrightarrow{a}$ extend as usual to *path* relations $\stackrel{u}{\Longrightarrow}$ for $u \in T^*$. Branching bisimulation [GW 89] is a refinement of strong bisimulation [Pa 81], introduced to cope with weak transitions $\xrightarrow{\epsilon}$ but nevertheless it strongly preserves the branching structure.

Definition 2.1 A *branching bisimulation* R on a graph G is a binary relation on the vertices of G satisfying the following two symmetrical conditions:

(i) if $p \; R \; q$ and $p \xrightarrow{a} p'$ then
  (i1) either $a = \epsilon$ and $p' \; R \; q$
  (i2) or there exist q', q'' such that $q \stackrel{\epsilon}{\Longrightarrow} q' \xrightarrow{a} q''$ with $p \; R \; q'$ and $p' \; R \; q''$,

(ii) if $p \; R \; q$ and $q \xrightarrow{a} q'$ then
  (ii1) either $a = \epsilon$ and $p \; R \; q'$
  (ii2) or there exist p', p'' such that $p \stackrel{\epsilon}{\Longrightarrow} p' \xrightarrow{a} p''$ with $p' \; R \; q$ and $p'' \; R \; q'$.

As the set of (branching) bisimulations on a graph G is closed under union (finite or infinite), there exists a greatest branching bisimulation $\equiv_G$ on G, defined as the union of all the branching bisimulations of G. Note that for finite graphs, branching bisimulation is decidable in polynomial time [GV 90]. In order to show that $\equiv_G$ is an equivalence, Van Glabbeek and Weijland [GW 89] use a weaker form of the following lemma.

Lemma 2.2 *Let* R *be a (branching) bisimulation on* G *then*
$[R] := \{ (p,q) \mid \exists\, p_0, p_1, q_0, q_1,\ p_0 \stackrel{\epsilon}{\Longrightarrow} p \stackrel{\epsilon}{\Longrightarrow} p_1 \wedge q_0 \stackrel{\epsilon}{\Longrightarrow} q \stackrel{\epsilon}{\Longrightarrow} q_1 \wedge p_0\ R\ q_1 \wedge p_1\ R\ q_0 \}$
is a bisimulation on G *containing* R *and* [[R]] = [R].

The import of Lemma 2.2 is to remedy the absence of an internal composition of bisimulations by the following substitute.

Lemma 2.3 *If* R *and* S *are bisimulations on a graph* G *then* [R] ∘ [S] *is also a bisimulation on* G.

Let us now consider graph reductions. For any graph G and for any equivalence relation R on the vertices of G, the *quotient* G/R of G by R is the graph obtained by identifying equivalent nodes and removing afterwards the ϵ-*loops*, i.e.

$$G/R \;=\; \{\ R(s) \stackrel{a}{\longrightarrow} R(t) \mid (s \stackrel{a}{\longrightarrow} t) \in G \ \wedge\ (R(s) = R(t) \implies a \neq \epsilon)\ \}\ ,$$

where $R(s)$ is the equivalence class of s.

Definition 2.4 The *canonical reduct* $G/\equiv$ of a graph G is its quotient by the greatest bisimulation $\equiv_G$.

In order to justify the above denotation, let us now introduce graph reduction.

Definition 2.5 A *reduction* h from a graph G to a graph H is a surjective mapping from the vertices of G to the vertices of H such that
(i) if $(p \stackrel{a}{\longrightarrow} p') \in G$ then $(a = \epsilon \ \wedge\ h(p) = h(p')) \ \vee\ (h(p) \stackrel{a}{\longrightarrow} h(p')) \in H$
(ii) if $(h(p) \stackrel{a}{\longrightarrow} q') \in H$ then there exist vertices p', p'' of G such that
$$p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p'' \ \wedge\ h(p) = h(p') \ \wedge\ h(p'') = q'.$$

Unlike branching bisimulation relations, the above reductions are closed under composition.

Lemma 2.6 a) *The composition of two reductions is a reduction.*
b) *If a reduction defined on a graph without* ϵ*-loop decomposes into a reduction followed by another mapping, that mapping is also a reduction.*

The above lemma is the crux for relating reductions and bisimulations, which makes sense in view of the following.

Lemma 2.7 **a)** *If* R *is a bisimulation equivalence on graph* G *then the canonical mapping of* R *is a reduction from* G *to* G/R.
b) *If* h *is a reduction from* G *to* H *then* Ker(h) *is a bisimulation equivalence on* G.

As an immediate consequence, bisimulation equivalences and kernels of reduction mappings are exactly the same for a fixed graph. It is worth noting that injective reductions suppress ϵ-loops and rename vertices. So, the h-reduct of a graph G is the factor of G by the kernel of h, up to the removal of ϵ-loops. More precisely, we have the following.

Lemma 2.8 *If* h *is a reduction from* G *to* H *then* h^{-1} *is an injective reduction from* H *to* G/Ker(h).

As a basis of Lemmas 2.6 to 2.8, we obtain the following reduction theorem.

Theorem 2.9 *The canonical reduct of a graph* G *is the (unique, up to a vertex renaming) irreducible graph produced from* G *by graph reduction.*

Although the canonical reduct of a finite graph is always a finite graph, the family of transition graphs of pushdown automata is not closed under canonical reduction [CM 90], but the family of (reduced) context-free processes is closed under quotient by the greatest strong bisimulation [Ca 90 a]. We will extend the latter result to branching bisimulation, and this is the purpose of the next section.

3 Canonical reducts of context-free processes

After the necessary definition, we show by an example that additional conditions must be imposed on context-free processes in order to get a family closed under maximal reduction. Sufficient conditions may be borrowed from Hüttel's paper [Hü 91] on the decision of branching bisimulation for cf-processes. Under those conditions, the underlying grammar of a context-free process may be transformed into an equivalent grammar whose context-free process is nothing but the canonical reduct of the former (Theorem 3.19). The transformation uses a crucial property of branching bisimulation: that equivalence is a finitely generated congruence (on words) whose generating equations $u = v$ are *alphabetic*, meaning that u (or v) is a letter (Theorem 3.14).
Let us proceed to fix some notations.

Definition 3.1 Given an alphabet N of *non-terminals* and an alphabet T of *terminals*, an *alphabetic system* P is a finite subset of $N \times T \cup \{\epsilon\} \times N^*$.
The *context-free process* generated from $p \in N^*$ along P is the graph:

$$p\overset{}{\underset{P}{\longmapsto}} := \{\, u \xrightarrow{a} v \mid u \overset{a}{\underset{P}{\longmapsto}} v \wedge p \overset{*}{\underset{P}{\longmapsto}} u \wedge a \in T \cup \{\epsilon\} \,\},$$

where $\overset{}{\underset{P}{\longmapsto}}^*$ is the reflexive and transitive closure of the *prefix rewriting* $\bigcup_a \overset{a}{\underset{P}{\longmapsto}}$ induced by P:

$$\overset{a}{\underset{P}{\longmapsto}} \;:=\; \{\, xv \xrightarrow{a} uv \mid (x \xrightarrow{a} u) \in P \;\wedge\; v \in N^* \,\}\,.$$

From [Ca 90 b], every context-free process is effectively an equational graph in the sense of [Co 90], that is we can transform an alphabetic system P and an axiom p into a deterministic graph grammar generating ${}_p\overset{}{\underset{P}{\longmapsto}}$. The canonical reduct of an equational graph needs not be equational [CM 90]. We will nevertheless try to prove the conjecture below.

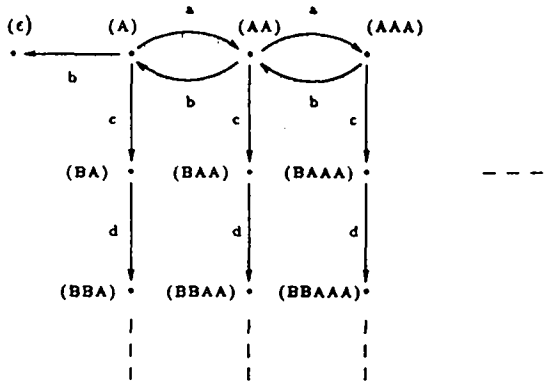
Conjecture 3.2 *The canonical reduct of a context-free process is an equational graph, and may be obtained by an effective construction.*

Since context-free processes are equational graphs, a stronger conjecture would be to state that the canonical reduct of a cf-process is always a cf-process. Unfortunately, this is false, and evidence of that failure is given by the following example.

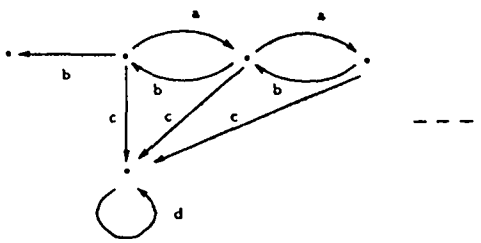
Example 3.3 Let

$$P \;=\; \{\, A \xrightarrow{a} AA \;,\; A \xrightarrow{b} \epsilon \;,\; A \xrightarrow{c} BA \;,\; B \xrightarrow{d} BB \,\}.$$

The context-free process ${}_A\overset{}{\underset{P}{\longmapsto}}$ generated from A is the following graph:



The canonical reduct of the above is the following graph:



but it has an infinite in-degree, and hence is not a context-free process.

A striking feature of the counter-example is the absence of "popping" transitions leading to the empty state ϵ, that is the cf-process is not reduced.

Definition 3.4 The *valuation* $\|u\|$ of a non-terminal word u is the smallest length of labels of the paths from u to ϵ if such a path exists, else is infinite, i.e.

$$\|u\| \;=\; min(\{\, |v| \mid u \stackrel{v}{\Longrightarrow} \epsilon \,\} \cup \{\infty\}) \,.$$

An alphabetic system is *reduced* if $\|x\|$ is finite for any non-terminal x, *proper* if $\|x\|$ always differs from zero.

By imposing reduced cf-processes (the underlying alphabetic systems are reduced), one may hope to keep a finite degree and thus prove Conjecture 3.2 specialized to the following.

Conjecture 3.5 *The canonical reduct of a reduced cf-process is a (reduced) cf-process, and may be obtained by an effective construction.*

This conjecture holds for strong bisimulation [Ca 90 a], [CM 90], but we were unable to prove it for branching bisimulation. Fortunately, Conjecture 3.2 is still entailed by a further specialization of Conjecture 3.5, restricted to proper (and reduced) cf-processes. The following series of lemmas and propositions state properties of reduced cf-processes. *Henceforth P is a reduced alphabetic system and $\equiv$ is the greatest branching bisimulation on the set-theoretic union of all the cf-processes $\stackrel{p}{\longmapsto}_P$ for $p \in N^*$.*
The next lemma, adapted from [Ca 90 a], was already stated in that form in [Hü 91].

Lemma 3.6 *For any non-terminal words* u,v,x,y,

a) *if* $u \equiv v$ *and* $x \equiv y$ *then* $ux \equiv vy$

b) *if* $u \equiv v$ *then* $\|u\| = \|v\|$

c) $\|uv\| = \|u\| + \|v\|$.

The above statement would be false in general without the proviso that P is a reduced alphabetic system, e.g. it is false if both c and d are replaced by ϵ in Example 3.3. Lemma 3.6 (a) states that the equivalence $\equiv$ is compatible w.r.t. concatenation, i.e. $\equiv$ is a *congruence*. Lemma 3.6 (b) states that $\equiv$ is *norm preserving*. Our next goal is to show that $\equiv$ is generated by a finite set of *alphabetic* equations $x_i = u_i$ where $x_i \in N$ and $v_i \in N^*$. For that purpose, let us recall the usual notations. Given a binary relation R on N^*, let $\underset{R}{\longrightarrow} = \{\, (xuy, xvy) \mid u \,R\, v \wedge x, y \in N^* \,\}$ be the rewriting according to R, and let $\underset{R}{\overset{*}{\longleftrightarrow}}$ be the congruence generated by R, i.e. the symmetric, reflexive and transitive closure of $\underset{R}{\longrightarrow}$. The following is variant form of the self-proving relations introduced in [Co 83], suitable for branching bisimulation.

Definition 3.7 A binary relation R on N^* is a *self-proving* relation (w.r.t. P) if $p\ R\ q$ implies the following conditions:

(i) $p \stackrel{\epsilon}{\Longrightarrow} \epsilon$ iff $q \stackrel{\epsilon}{\Longrightarrow} \epsilon$

(ii) if $p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$ then

(ii1) either $a = \epsilon$ and there exists q' such that
$q \stackrel{\epsilon}{\Longrightarrow} q'$ with $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$

(ii2) or there exist q', q'' such that
$q \stackrel{\epsilon}{\Longrightarrow} q' \stackrel{a}{\longrightarrow} q''$ with $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''$

(iii) if $q \stackrel{\epsilon}{\Longrightarrow} q' \stackrel{a}{\longrightarrow} q''$ then

(iii1) either $a = \epsilon$ and there exists p' such that
$p \stackrel{\epsilon}{\Longrightarrow} p'$ with $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''$

(iii2) or there exist p', p'' such that
$p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$ with $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''$.

A glance at Definition 2.1 shows a strong similarity with the definition of branching bisimulation. Nevertheless, transitions $p \stackrel{a}{\longrightarrow} q$ have been extended to sequences of transitions $p \stackrel{\epsilon}{\Longrightarrow} \stackrel{a}{\longrightarrow} p'$, and the recursive occurrences of R have been replaced by $\stackrel{*}{\underset{R}{\longleftrightarrow}}$. Those disparities are significant since self-proving relations are generally not bisimulations, although the converse inclusion is true.

Lemma 3.8 a) *Every bisimulation is a self-proving relation.*
b) *Every self-proving congruence is a bisimulation.*

The notion of self-proving relation generalizes and simplifies the notion of branching bisimulation up to sequential congruence introduced in [Hü 91], and has moreover the advantage to cover all systems of generators for bisimulation, which is precisely expressed by the proposition below.

Proposition 3.9 *A relation* R *is self-proving if and only if its least congruence* $\stackrel{*}{\underset{R}{\longleftrightarrow}}$ *is a bisimulation.*

In view of the above, any generating system for branching bisimulation $\equiv$ on a reduced cf-process must be a self-proving relation. Nevertheless, the generating systems we have in mind are finite systems of alphabetic equations. Under the assumption that cf-processes are not only reduced but also proper (Definition 3.4), we are able to produce alphabetic systems that generate branching bisimulation. The end of the paper presents the construction.

It is always assumed from now on that P is a proper (and reduced) alphabetic system.

In a first stage, let us prove the existence of alphabetic systems generating branching bisimulation, without paying attention to their construction. For that purpose, we need to introduce the notion of basic relation.

Definition 3.10 A binary relation R on N^+ is a *basic relation* if it fulfills the three following conditions:

(i) R is functional: $x\ R\ u \wedge x\ R\ v \implies u = v$

(ii) R is alphabetic: $Dom(R) \subseteq N$

(iii) R is "eventually irreducible": every x in $Dom(R)$ reduces along R to an irreducible word.

Lemma 3.11 *If* R *is a basic relation then*

a) R *is finite*

b) *the rewriting relation* $\underset{R}{\longrightarrow}$ *is terminating and confluent;*
thus any word u *reduces along* R *to a unique normal form* u$\downarrow$R.

The following lemma shows that the greatest branching bisimulation $\equiv$ can be decomposed by words with the same norm.

Lemma 3.12 *If* su $\equiv$ tv *with* $\|s\| = \|t\|$ *then* s $\equiv$ t *and* u $\equiv$ v.

This decomposition lemma can be extended to the following splitting lemma.

Lemma 3.13 *If* su $\equiv$ tv *with* $\|s\| \geq \|t\|$ *then* s $\equiv$ tw *and* wu $\equiv$ v *for some* w.

Remark that $AB \equiv B$ but $A \not\equiv \epsilon$ for the following reduced but not proper alphabetic system P:

$$P = \{ A \xrightarrow{\epsilon} \epsilon\ ,\ A \xrightarrow{a} \epsilon\ ,\ B \xrightarrow{\epsilon} \epsilon\ ,\ B \xrightarrow{a} AB \}\ ,$$

which shows the import of assuming proper systems.
Thus, there always exist basic systems generating the bisimulation. A finer characterization of those basic systems is provided by the following theorem.

Theorem 3.14 *Among the basic and self-proving relations, those that are maximal for inclusion generates the branching bisimulation* $\equiv$.

For deciding bisimulation, a restricted version is sufficient.

Corollary 3.15 u $\equiv$ v *iff* u$\downarrow$R = v$\downarrow$R *for some basic and self-proving relation* R.

We will now complete the technical development by giving an effective construction of the finite set of all basic and self-proving relations for a given reduced and proper alphabetic system P. Then, Theorem 3.14 indicates an effective construction of a basic generating system of bisimulation. The next statement is a transcription of Definition 3.7 adapted to the case where R is a basic relation. In that case, $u \overset{*}{\underset{R}{\longleftrightarrow}} v$ may be replaced by $u\downarrow R = v\downarrow R$,

and there suffices to consider for each word xv the transitions $xv \xrightarrow{a} x'v$ where $x \xrightarrow{a} x'$ is a rule of the alphabetic system P. That lemma is crucial to obtain an effective and efficient construction of generating systems. We need the prefix order $\leq$ on N^*: $u \leq v$ if there exists w such that $uw = v$, and we write $v/u = w$.

Lemma 3.16 *A basic relation* R *is self-proving (w.r.t.* P*) if and only if for all* $y \in N$ *and for all* $(x \xrightarrow{a} x') \in P$ *with* $(a \neq \epsilon$ *or* $x{\downarrow}R \neq x'{\downarrow}R)$*, the two following conditions are satisfied:*

(i) if $x{\downarrow}R \leq y{\downarrow}R$ *then there exist* y', y'' *such that*
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ *with* $y{\downarrow}R = y'{\downarrow}R$ *and* $(y{\downarrow}R)/(x{\downarrow}R) = (y''{\downarrow}R)/(x'{\downarrow}R)$

(ii) if $x{\downarrow}R > y{\downarrow}R$ *then there exist* y', y'' *such that*
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ *with* $y{\downarrow}R = y'{\downarrow}R$ *and* $(x{\downarrow}R)/(y{\downarrow}R) = (x'{\downarrow}R)/(y''{\downarrow}R)$.

The basic self-proving relations are the successful functions introduced in [CHT 92]. On the basis of Lemma 3.16 and with the help of Büchi's results on "regular canonical systems" [Bü 64], we obtain the following proposition.

Proposition 3.17 *One may decide whether a basic relation is self-proving.*

Because the set of basic systems is finite and constructible, Theorem 3.14 and Proposition 3.17 indicate an effective procedure which, given a proper and reduced alphabetic system P, produces a basic system generating the associated bisimulation $\equiv$. In view of Lemma 3.11, we have as a by-product the result of [Hü 91].

Corollary 3.18 *For every proper and reduced alphabetic system, the branching bisimulation is decidable.*

The main result of the present paper is the following theorem.

Theorem 3.19 *Given a proper and reduced alphabetic system* P *and an axiom* p*, one can effectively construct a proper and reduced alphabetic system* Q *and an axiom* q *such that:*

a) *the context-free process* $\longmapsto_{q_Q}$ *is isomorphic to the quotient of the context-free process* $\longmapsto_{p_P}$ *by its greatest branching bisimulation,*

b) *the union of all the cf-processes of* Q *is isomorphic to the quotient of the union of all the cf-processes of* P *by its greatest branching bisimulation.*

More precisely, Theorem 3.19 is proved by defining

$$Q = \{\, x{\downarrow}R \xrightarrow{a} u{\downarrow}R \mid (x \xrightarrow{a} u) \in P \ \wedge\ |x{\downarrow}R| = 1 \ \wedge\ (x{\downarrow}R = u{\downarrow}R \implies a \neq \epsilon) \,\},$$

where R is any basic system generating $\equiv$, and point (a) of Theorem 3.19 then follows from point (b). To sum up, we have shown that the quotient of a reduced and proper cf-process by its greatest branching bisimulation is still a reduced and proper cf-process, which was our assigned objective. It follows that both Conjecture 3.2 and Conjecture 3.5 hold for reduced and proper cf-processes.

4 Complexity upper bound

We show the existence of a maximal basic self-proving relation of polynomial length. From Lemma 3.16, we deduce a Σ_2^p algorithm to decide whether a basic relation is self-proving. From this, we obtain a Σ_2^p complexity upper bound for deciding branching bisimulation for reduced and proper cf-processes (Theorem 4.9). Furthermore, we deduce an algorithm in Σ_3^p to extract a maximal basic and self-proving relation. Then, any alphabetic system may be transformed in PSPACE into an equivalent canonical alphabetic system (Theorem 4.11).

First, we give a polynomial bound for $|v| - |u|$ if there exists a *norm-non-increasing path* $u \Downarrow v$ from u to v, i.e. a sequence $u = u_0, \ldots, u_k = v$ of non-terminal words such that $u_i \underset{P}{\longmapsto} u_{i+1}$ and $\|u_i\| \geq \|u_{i+1}\|$ for every $0 \leq i < k$. This bound is expressed according to the number $n = \#\{ u(i) \mid u \in Dom(P) \cup Im(P) \wedge 1 \leq i \leq |u| \}$ of non-terminals in P, and to the maximal length $m = max\{ |u| \mid u \in Dom(P) \cup Im(P) \}$ of the words in P.

Lemma 4.1 *If* $u \Downarrow v$ *then* $|v| \leq |u| + (n-1)(m-1)$.

From Lemma 2.2 and Lemma 3.6 (b), every ϵ-path between bisimilar words is a norm-non-increasing path, so Lemma 4.1 can be applied.

Corollary 4.2 *If* $u \stackrel{\epsilon}{\Longrightarrow} v$ *and* $u \equiv v$ *then* $|v| \leq |u| + (n-1)(m-1)$.

Another consequence of Lemma 4.1 is that every non-empty class $[x]_R - \{x\} = \{ u \neq x \mid x \; R \; u \}$ of a letter x according to a bisimulation equivalence R, has a representative of polynomial length.

Lemma 4.3 *Given a bisimulation* R *and* $x \; R \; yu$ *with* $x, y \in N$, $u \in N^*$, *there exists* v *such that* $v \; R \; u$ *and* $|v| \leq (n-1)(m-1)+1$.

This lemma allows us to restrict Theorem 3.14 to basic and self-proving relations R of polynomial length $|R| = max\{ |u| \mid u \in Im(R) \}$.

Proposition 4.4 *There exists a basic self-proving relation* R, *maximal w.r.t. inclusion of length* $|R| \leq (n-1)(m-1)+2$.

Then, we can restrict Corollary 3.15 to basic self-proving relations of polynomial length.

Corollary 4.5 $u \equiv v$ *iff* $u{\downarrow}R = v{\downarrow}R$ *for some basic self-proving relation* R *of length* $|R| \leq (n-1)(m-1)+2$.

This corollary is used to obtain a complexity upper bound for deciding branching bisimulation. First, we test in polynomial time that a binary relation is basic.

Lemma 4.6 *Given a functional relation* R *in* $N \times N^+$, *the problem of deciding whether* R *is basic is in* P.

Then, we give a co-NP upper bound for deciding the equality of normal forms w.r.t. a basic relation, or more generally and as needed in Lemma 3.16, for the prefix order of left quotients.

Lemma 4.7 *Given a basic relation* R *and non-terminal words* x, y, u, v, *the problem of deciding whether* $(x{\downarrow}R)/(y{\downarrow}R) \leq (u{\downarrow}R)/(v{\downarrow}R)$ *is in* co-NP.

Thus, the self-provability of a basic relation is decidable in $\Sigma_2^p = \mathrm{NP}^{\mathrm{NP}}$, that is with a polynomial time bounded nondeterministic Turing machine with an NP oracle [St 77].

Proposition 4.8 *The problem of deciding whether a basic relation is self-proving is in* Σ_2^p.

The Σ_2^p complexity for deciding strong bisimulation of reduced cf-processes [HT 92], is then extended to branching bisimulation.

Theorem 4.9 *The problem of deciding branching bisimulation for reduced and proper cf-processes is in* Σ_2^p.

This theorem with Proposition 4.4 permit to extract a generating system of bisimulation $\equiv$ by a $\Sigma_3^p = \mathrm{NP}^{\Sigma_2^p}$ algorithm, that is with a polynomial time bounded nondeterministic Turing machine with an Σ_2^p oracle [St 77].

Proposition 4.10 *There exists a* Σ_3^p *algorithm for computing a maximal (w.r.t. inclusion) basic self-proving relation.*

So, the construction of Theorem 3.19 may be done in Σ_3^p, even though the obtained canonical system may be of exponential length.

Theorem 4.11 *Minimization of reduced and proper cf-processes is in* PSPACE.

Acknowledgements

Let me thank P. Darondeau for his help in the drafting of this paper.

References

[BBK 87] J. BAETEN, J. BERGSTRA and J. KLOP *Decidability of bisimulation equivalence for processes generating context-free languages*, PARLE 87, LNCS 259, pp. 94–111, 1987.

[BK 88] J. BERGSTRA and J. KLOP *Process theory based on bisimulation semantics*, LNCS 354, pp. 50–122, 1988.

[Bü 64] R. BÜCHI *Regular canonical systems*, Archiv für Mathematische Logik und Grundlagenforschung 6, pp. 91–111, 1964.

[Ca 90 a] D. CAUCAL *Graphes canoniques de graphes algébriques*, RAIRO-TIA 24-4, pp. 339–352, 1990.

[Ca 90 b] D. CAUCAL *On the regular structure of prefix rewriting*, CAAP 90, LNCS 431, pp. 87–102, 1990, an extended version will appear in TCS A, Vol. 106, 1993.

[CHT 92] D. CAUCAL, D. HUYNH and L. TIAN *Deciding branching bisimilarity of normed context-free processes is in* Σ_2^p, Technical Report UTDCS-8-92, 1992.

[CM 90] D. CAUCAL and R. MONFORT *On the transition graphs of automata and grammars*, WG 90, LNCS 484, pp. 311–337, 1990.

[Co 83] B. COURCELLE *An axiomatic approach to the* KH *algorithms*, Mathematical System Theory 16, pp. 191–231, 1983.

[Co 90] B. COURCELLE *Graph rewriting: an algebraic and logic approach*, Handbook of TCS, Vol. B, Elsevier, pp. 193–242, 1990.

[GW 89] R. VAN GLABBEEK and P. WEIJLAND *Branching time and abstraction in bisimulation semantics*, Proceedings 11^{th} IFIP World Computer Congress, 1989.

[GV 89] J. GROOTE and F. VAANDRAGER *Structured operational semantics and bisimulation as a congruence*, ICALP 89, LNCS 372, pp. 423–438, 1989.

[GV 90] J. GROOTE and F. VAANDRAGER *An efficient algorithm for branching bisimulation and stuttering equivalence*, ICALP 90, LNCS 443, pp. 626–638, 1990.

[Hü 91] H. HÜTTEL *Silence is golden: branching bisimilarity is decidable for context-free processes*, CAV 91, LNCS 575, pp. 2–12, 1991.

[HS 91] H. HÜTTEL and C. STIRLING *Actions speak louder than words: proving bisimilarity for context-free processes*, LICS 91, to appear, 1991.

[HT 92] D. HUYNH and L. TIAN *Deciding bisimilarity of normed context-free processes is in* Σ_2^p, Technical Report UTDCS-1-92, to appear in TCS, 1992.

[Pa 81] D. PARK *Concurrency and automata on infinite sequences*, LNCS 104, pp. 167–183, 1981.

[St 77] L. STOCKMEYER *The polynomial time hierarchy*, TCS 3, pp. 1–22, 1977.

Appendix

We give here all the proofs of this paper.

Lemma 2.2 *Let* R *be a (branching) bisimulation on* G *then*
$[R] := \{ (p,q) \mid \exists\, p_0, p_1, q_0, q_1,\ p_0 \stackrel{\epsilon}{\Longrightarrow} p \stackrel{\epsilon}{\Longrightarrow} p_1 \wedge q_0 \stackrel{\epsilon}{\Longrightarrow} q \stackrel{\epsilon}{\Longrightarrow} q_1 \wedge p_0\ R\ q_1 \wedge p_1\ R\ q_0 \}$
is a bisimulation on G *containing* R *and* [[R]] = [R].

Proof.
i) By definition $R \subseteq [R]$. Let us show that $[R]$ is a bisimulation of G.
As R is a bisimulation and by symmetry of $[R]$, it suffices to show point (i) of Definition 2.1 for $p\ [R] - R\ q$ and $p \stackrel{a}{\longrightarrow} p'$. By definition of $[R]$, there exist p_0, p_1, q_0, q_1 such that

$$p_0 \stackrel{\epsilon}{\Longrightarrow} p \stackrel{\epsilon}{\Longrightarrow} p_1\ ,\ q_0 \stackrel{\epsilon}{\Longrightarrow} q \stackrel{\epsilon}{\Longrightarrow} q_1\ ,\ p_0\ R\ q_1 \text{ and } p_1\ R\ q_0.$$

As $p_0\ R\ q_1$ and by induction on the length of the derivation $p_0 \stackrel{\epsilon}{\Longrightarrow} p$, there exists q' such that $q_1 \stackrel{\epsilon}{\Longrightarrow} q'$ and $p\ R\ q'$. As $p\ R\ q'$, $p \stackrel{a}{\longrightarrow} p'$ and R is a bisimulation, one of the two cases below applies:

Case 1: $a = \epsilon$ and $p'\ R\ q'$.
By hypothesis $p\ [R] - R\ q$ hence $q' \neq q$.
As $q \stackrel{\epsilon}{\Longrightarrow} q'$, there exists q'' such that $q \stackrel{\epsilon}{\Longrightarrow} q'' \stackrel{\epsilon}{\longrightarrow} q'$.
As $p \stackrel{\epsilon}{\Longrightarrow} p \stackrel{\epsilon}{\Longrightarrow} p_1$, $q_0 \stackrel{\epsilon}{\Longrightarrow} q'' \stackrel{\epsilon}{\longrightarrow} q'$, $p\ R\ q'$, $p_1\ R\ q_0$, we have $p\ [R]\ q''$.
Hence $p\ [R] - R\ q$ satisfies condition (i2) of Definition 2.1.

Case 2: there exist r, s such that $q' \stackrel{\epsilon}{\Longrightarrow} r \stackrel{a}{\longrightarrow} s$ with $p\ R\ r$ and $p'\ R\ s$.
So $q \stackrel{\epsilon}{\Longrightarrow} r$ hence $p\ [R] - R\ q$ satisfies condition (i2) of Definition 2.1.

ii) Let us show that $[[R]] = [R]$.
Let $p\ [[R]]\ q$. There exist p_0, p_1, q_0, q_1 such that

$$p_0 \stackrel{\epsilon}{\Longrightarrow} p \stackrel{\epsilon}{\Longrightarrow} p_1\ ,\ q_0 \stackrel{\epsilon}{\Longrightarrow} q \stackrel{\epsilon}{\Longrightarrow} q_1\ ,\ p_0\ [R]\ q_1 \text{ and } p_1\ [R]\ q_0.$$

As $p_0\ [R]\ q_1$, there exist p_0', q_1' such that $p_0' \stackrel{\epsilon}{\Longrightarrow} p_0$, $q_1 \stackrel{\epsilon}{\Longrightarrow} q_1'$ and $p_0'\ R\ q_1'$.
As $p_1\ [R]\ q_0$, there exist p_1', q_0' such that $p_1 \stackrel{\epsilon}{\Longrightarrow} p_1'$, $q_0' \stackrel{\epsilon}{\Longrightarrow} q_0$ and $p_1'\ R\ q_0'$.
Thus $p_0' \stackrel{\epsilon}{\Longrightarrow} p \stackrel{\epsilon}{\Longrightarrow} p_1'$, $q_0' \stackrel{\epsilon}{\Longrightarrow} q \stackrel{\epsilon}{\Longrightarrow} q_1'$, $p_0'\ R\ q_1'$ and $p_1'\ R\ q_0'$.
Hence $p\ [R]\ q$. Finally $[[R]] \subseteq [R] \subseteq [[R]]$, hence the equality.
□

Lemma 2.3 *If* R *and* S *are bisimulations on a graph* G *then* [R] ∘ [S] *is also a bisimulation on* G.

Proof.
By symmetry of R and S, it suffices to show condition (i) of Definition 2.1 for $p\ [R] \circ [S]\ q$ and $p \stackrel{a}{\longrightarrow} p'$.
There exists r such that $p\ [R]\ r\ [S]\ q$. From Lemma 2.2, $[R]$ is a bisimulation and we have one of the two cases below.

Case 1: $a = \epsilon$ and $p'\ [R]\ r$.
So $p'\ [R] \circ [S]\ q$ hence $p\ [R] \circ [S]\ q$ satisfies condition (i1) of Definition 2.1.

Case 2: there exist r' and r'' such that $r \stackrel{\epsilon}{\Longrightarrow} r' \stackrel{a}{\longrightarrow} r''$ with $p\ [R]\ r'$ and $p'\ [R]\ r''$.

From Lemma 2.2, $[S]$ is a bisimulation. By induction on the derivation length of $r \stackrel{\epsilon}{\Longrightarrow} r'$, there exist $n \geq 0$ and two sequences $r_0, r'_0, \ldots, r_n, r'_n$ and $q_0, q'_0, \ldots, q'_{n-1}, q_n$ such that

$r_0 = r$ and $q_0 = q$, $r'_n = r'$,

$r_i \stackrel{\epsilon}{\Longrightarrow} r'_i$ and $q_i \stackrel{\epsilon}{\Longrightarrow} q'_i$, $r'_i \stackrel{\epsilon}{\longrightarrow} r_{i+1}$ and $q'_i \stackrel{\epsilon}{\longrightarrow} q_{i+1}$,

$r_i\ [S]\ q_i$ and $r'_i\ [S]\ q_i$, $r'_i\ [S]\ q'_i$.

As $r' = r'_n\ [S]\ q_n$ and $r' \stackrel{a}{\longrightarrow} r''$, we have one of the two cases below.

Case 2.1: $a = \epsilon$ and $r''\ [S]\ q_n$.

If $n = 0$ then $q_n = q$ hence $p'\ [R] \circ [S]\ q$;

thus $p\ [R] \circ [S]\ q$ satisfies condition (i1) of Definition 2.1.

If $n \neq 0$ then $r \stackrel{\epsilon}{\Longrightarrow} r'_{n-1} \stackrel{\epsilon}{\Longrightarrow} r'$, $r'_{n-1}\ [S]\ q'_{n-1}$, $q'_{n-1} \stackrel{\epsilon}{\longrightarrow} q_n$.

From Lemma 2.2, $[[R]] = [R]$. Furthermore $p\ [R]\ r$ and $p\ [R]\ r'$.

In consequence $p\ [R]\ r'_{n-1}$ hence $p\ [R] \circ [S]\ q'_{n-1}$.

Thus $p\ [R] \circ [S]\ q$ satisfies condition (i2) of Definition 2.1.

Case 2.2: there exist q', q'' such that $q_n \stackrel{\epsilon}{\Longrightarrow} q' \stackrel{a}{\longrightarrow} q''$, $r'\ [S]\ q'$ and $r''\ [S]\ q''$.

Thus $q \stackrel{\epsilon}{\Longrightarrow} q' \stackrel{a}{\longrightarrow} q''$, $p\ [R] \circ [S]\ q'$ and $p'\ [R] \circ [S]\ q''$.

Hence $p\ [R] \circ [S]\ q$ satisfies condition (i2) of Definition 2.1.

Finally $[R] \circ [S]$ is a bisimulation of G.

□

Lemma 2.6 a) *The composition of two reductions is a reduction.*

b) *If a reduction defined on a graph without ϵ-loop decomposes into a reduction followed by another mapping, that mapping is also a reduction.*

Proof.

i) Let g be a reduction from a graph G to a graph H, and let h be a reduction from H to a graph K. Let us show that $g \circ h$ (where $(g \circ h)(x) = h(g(x))$) is a reduction.

The composition of two surjective mappings is a surjective mapping. Let us prove that $g \circ h$ satisfies (i) of Definition 2.5.

Consider an arc $p \stackrel{a}{\longrightarrow} p'$ of G. As g satisfies condition (i) of Definition 2.5, one of the two cases below applies.

Case 1: $a = \epsilon$ and $g(p) = g(p')$. Thus $h(g(p)) = h(g(p'))$.

Case 2: $g(p) \stackrel{a}{\longrightarrow} g(p')$ is an arc of H.

As h satisfies (i) of Definition 2.5, we have one of the two following subcases.

Case 2.1: $a = \epsilon$ and $h(g(p)) = h(g(p'))$.

Case 2.2: $h(g(p)) \stackrel{a}{\longrightarrow} h(g(p'))$ is an arc of K.

In all cases, $g \circ h$ satisfies condition (i) of Definition 2.5.

Let us prove that $g \circ h$ satisfies (ii) of Definition 2.5.

Let $h(g(p)) \stackrel{a}{\longrightarrow} r$ be an arc of K. As h satisfies (ii) of 2.5, there are vertices q and q' of H such that

$$g(p) \stackrel{\epsilon}{\Longrightarrow} q \stackrel{a}{\longrightarrow} q' \quad \text{with} \quad h(q) = h(g(p)) \text{ and } h(q') = r.$$

As g satisfies point (ii) of 2.5 and by induction on the derivation length of $g(p) \stackrel{\epsilon}{\Longrightarrow} q$, there exists r such that $p \stackrel{\epsilon}{\Longrightarrow} r$ and $g(r) = q$. As $g(r) \stackrel{a}{\longrightarrow} q'$ and g satisfies (ii) of 2.5, there exist p' and p'' such that

$$r \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p'' \text{ with } g(p') = g(r) \text{ and } g(p'') = q'.$$

Finally $p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$ with $h(g(p')) = h(g(r)) = h(q) = h(g(p))$ and $h(g(p'')) = h(q') = r$.
Thus $g \circ h$ satisfies condition (ii) of Definition 2.5.

ii) Let g be a reduction from a graph G to a graph H, and let h be a mapping from H to a graph K without ϵ-loop (i.e. for every vertex p, $p \stackrel{\epsilon}{\longrightarrow} p$ is not an arc of K) such that $g \circ h$ is a reduction. Let us show that h is a reduction.
Let us prove that h satisfies point (i) of Definition 2.5 .
Let $r \stackrel{a}{\longrightarrow} r'$ be an arc of H. As g is surjective, there exists p such that $g(p) = r$.
As $g(p) \stackrel{a}{\longrightarrow} r'$ and g satisfies (ii) of 2.5, there exist p' and p'' such that

$$p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p'' \text{ with } g(p') = g(p) \text{ and } g(p'') = r'.$$

As $g \circ h$ is a reduction and $p' \stackrel{a}{\longrightarrow} p''$, we have one of the two cases below.

Case 1: $a = \epsilon$ and $h(g(p')) = h(g(p''))$.
Thus $h(r) = h(g(p)) = h(g(p')) = h(g(p'')) = h(r')$.

Case 2: $h(g(p')) \stackrel{a}{\longrightarrow} h(g(p''))$ is an arc of K, i.e. $h(r) \stackrel{a}{\longrightarrow} h(r')$ is an arc of K.

Thus h satisfies (i) of 2.5.
Let us prove that h satisfies (ii) of 2.5.
Let $h(r) \stackrel{a}{\longrightarrow} r'$ be an arc of K. As g is surjective, there exists p such that $g(p) = r$.
As $h(g(p)) \stackrel{a}{\longrightarrow} r'$ and $g \circ h$ satisfies (ii) of 2.5, there exist p' and p'' such that

$$p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p'' \text{ with } h(g(p')) = h(g(p)) \text{ and } h(g(p'')) = r'.$$

As g is a reduction and $p' \stackrel{a}{\longrightarrow} p''$, one of the two cases below applies.

Case 1: $a = \epsilon$ and $g(p') = g(p'')$.
Then $h(r) = h(g(p)) = h(g(p')) = h(g(p'')) = r'$. Hence $h(r) \stackrel{a}{\longrightarrow} r'$ is an ϵ-loop of K, which is forbidden by hypothesis.

Case 2: $g(p') \stackrel{a}{\longrightarrow} g(p'')$ is an arc of H.
As g satisfies (i) of 2.5 and by induction on the derivation length of $p \stackrel{\epsilon}{\Longrightarrow} p'$, we have $g(p) \stackrel{\epsilon}{\Longrightarrow} g(p')$. Thus

$$r \stackrel{\epsilon}{\Longrightarrow} g(p') \stackrel{a}{\longrightarrow} g(p'') \text{ with } h(g(p')) = h(g(p)) = h(r) \text{ and } h(g(p'')) = r'.$$

Finally h satisfies condition (ii) of Definition 2.5.
□

Lemma 2.7 a) *If* R *is a bisimulation equivalence on graph* G *then the canonical mapping of* R *is a reduction from* G *to* G/R.
b) *If* h *is a reduction from* G *to* H *then* Ker(h) *is a bisimulation equivalence on* G.

Proof.
i) Let R be a (branching) bisimulation on a graph G such that R is an equivalence on the set of vertices of G. We denote by π_R the canonical mapping $G \longrightarrow G/R$, i.e. $\pi_R(x) = R(x) = \{ y \mid x \; R \; y \}$ is the equivalence class of any vertex x according to R. Let us show that π_R is a reduction from G to G/R.

Let us prove that π_R satisfies condition (i) of Definition 2.5.
Consider an arc $p \xrightarrow{a} p'$ of G. As R is reflexive, we have $p\ R\ p$. As R is a bisimulation, we have one of the two cases below.

Case 1: $a = \epsilon$ and $p'\ R\ p$. Thus $\pi_R(p) = \pi_R(p')$.

Case 2: There exist q and q' such that $p \stackrel{\epsilon}{\Longrightarrow} q \xrightarrow{a} q'$ with $p\ R\ q$ and $p'\ R\ q'$.

Either $\pi_R(p) = \pi_R(p')$ and $a = \epsilon$.

Or $\pi_R(p) = \pi_R(q) \xrightarrow{a} \pi_R(q') = \pi_R(p')$ is an arc of G/R.

In all cases, π_R satisfies (i) of 2.5.
Let us prove that π_R satisfies condition (ii) of Definition 2.5.
Let $\pi_R(p) \xrightarrow{a} q'$ be an arc of G/R. By definition of G/R, there exists an arc $r \xrightarrow{a} r'$ of G such that $r\ R\ p$ and $\pi_R(r') = q'$. Furthermore, the case $a = \epsilon \ \wedge \ q' = \pi_R(p)$ is excluded, i.e. it is not possible to have $a = \epsilon$ with $r'\ R\ p$. As R is a bisimulation, there must exist p' and p'' such that

$$p \stackrel{\epsilon}{\Longrightarrow} p' \xrightarrow{a} p'' \text{ with } r\ R\ p' \text{ and } r'\ R\ p''.$$

So $\pi_R(p) = \pi_R(r) = \pi_R(p')$ and $\pi_R(p'') = \pi_R(r') = q'$.
So π_R satisfies condition (ii) of Definition 2.5.

ii) Let h be a reduction from a graph G to a graph H. The kernel

$$Ker(h) = \{\ (p, q) \mid h(p) = h(q)\ \}$$

of h is an equivalence on the vertices of G. Let us prove that $Ker(h)$ is a bisimulation of G.
Consider an arc $p \xrightarrow{a} p'$ of G and let q be a vertex such that $h(p) = h(q)$. As h satisfies condition (i) of Definition 2.5, we have one of the two cases below.

Case 1: $a = \epsilon$ and $h(p) = h(p')$.

Hence $a = \epsilon$ and $h(q) = h(p')$.

Thus $p\ Ker(h)\ q$ satisfies condition (i1) of Definition 2.1.

Case 2: $h(p) \xrightarrow{a} h(p')$ is an arc of H.

So $h(q) \xrightarrow{a} h(p')$ and as h satisfies (ii) of 2.5, there exist q' and q'' such that

$$q \stackrel{\epsilon}{\Longrightarrow} q' \xrightarrow{a} q'' \text{ with } h(q) = h(q') \text{ and } h(q'') = h(p').$$

Thus $p\ Ker(h)\ q'$ and $p'\ Ker(h)\ q''$.

Hence $p\ Ker(h)\ q$ satisfies (i2) of Definition 2.1.

As $Ker(h)$ is symmetric, it follows that $Ker(h)$ is a bisimulation of G.
□

Lemma 2.8 *If* h *is a reduction from* G *to* H *then* h^{-1} *is an injective reduction from* H *to* G/Ker(h).

Proof.
Let h be a reduction from a graph G to a graph H. For every vertex p of G,

$$h^{-1}(h(p)) \ = \ \{\ q \mid h(q) = h(p)\ \}$$

is the equivalence class of p according to $Ker(h)$. Thus h^{-1} is a bijection from the set of vertices of H to the set of vertices of $G/Ker(h)$.
From Lemma 2.7, $h \circ h^{-1} = \pi_{Ker(h)}$ is a reduction. From Lemma 2.6 (b), h^{-1} is a reduction.
□

Theorem 2.9 *The canonical reduct of a graph* G *is the (unique, up to a vertex renaming) irreducible graph produced from* G *by graph reduction.*

Proof.

i) Let us show that $G/\equiv$ is reducible from G and is irreducible.
From Lemma 2.3, $\equiv$ is an equivalence. From Lemma 2.7, $\pi_{\equiv}$ is a reduction from G to $G/\equiv$, hence $G/\equiv$ is reducible from G.
Let h be a reduction from $G/\equiv$ to a graph H. From Lemma 2.6 (a), $\pi_{\equiv} \circ h$ is a reduction from G to H. From Lemma 2.7 (b), $Ker(\pi_{\equiv} \circ h)$ is a bisimulation of G containing $Ker(\pi_{\equiv}) = \equiv$. By maximality of $\equiv$, $Ker(\pi_{\equiv} \circ h) = Ker(\pi_{\equiv})$, i.e. h is injective. As $G/\equiv$ is without ϵ-loop, H is isomorphic to $G/\equiv$. Finally $G/\equiv$ is irreducible.

ii) Consider a reduction h from a graph G to an irreducible graph H, i.e. H is only reducible to graphs isomorphic to H. Let us prove that H is isomorphic to $G/\equiv$.
From Lemma 2.7, $Ker(h) \subseteq \equiv$ and $\pi_{Ker(h)}$ is a reduction from G to $G/Ker(h)$.
As $Ker(h) \subseteq \equiv$, there exists a mapping g from $G/Ker(h)$ to $G/\equiv$ such that

$$\pi_{Ker(h)} \circ g = \pi_{\equiv}.$$

From Lemma 2.6 (b), g is a reduction. From Lemma 2.8 and Lemma 2.6 (a), $h^{-1} \circ g$ is a reduction from H to $G/\equiv$.
As H is irreducible, H is isomorphic to $G/\equiv$.
□

Lemma 3.6 *For any non-terminal words* u,v,x,y,

a) *if* u ≡ v *and* x ≡ y *then* ux ≡ vy
b) *if* u ≡ v *then* ||u|| = ||v||
c) ||uv|| = ||u|| + ||v|| .

Proof.

i) Let us prove (b). As $\equiv$ is a bisimulation, we have the following property:

if $u \equiv v$ and $u \stackrel{w}{\Longrightarrow} u'$ then there exists v' such that $v \stackrel{w}{\Longrightarrow} v'$ and $u' \equiv v'$. (1)

Let $u \equiv v$. As P is reduced, there exists w such that $u \stackrel{w}{\Longrightarrow} \epsilon$. From (1), there exists v' such that $v \stackrel{w}{\Longrightarrow} v'$ and $\epsilon \equiv v'$. As P is reduced, there exists w' such that $v' \stackrel{w'}{\Longrightarrow} \epsilon$. By symmetry of $\equiv$ and from (1), $w' = \epsilon$. Thus $v \stackrel{w}{\Longrightarrow} \epsilon$. Consequently $\|v\| \leq \|u\|$ and by symmetry of $\equiv$, we obtain $\|u\| = \|v\|$.

ii) To prove (a), it suffices to show that the relation

$$R = \{ (ux, vy) \mid u \equiv v \ \wedge \ x \equiv y \}$$

is a (branching) bisimulation of $\bigcup_p \stackrel{p}{\longmapsto}_P$.
Let $u \equiv v$, $x \equiv y$ and $ux \stackrel{a}{\longrightarrow} w$. We have one of the two cases below.

Case 1: $u \neq \epsilon$.

So, there exists u' such that $u \stackrel{a}{\longrightarrow} u'$ and $w = u'x$.

As $u \equiv v$ and $u \xrightarrow{a} u'$, one of the two cases below applies.

Case 1.1: $a = \epsilon$ and $u' \equiv v$.

Then $w = u'x \; R \; vy$. Hence $ux \; R \; vy$ satisfies point (i1) of Definition 2.1 .

Case 1.2: there exist v' and v'' such that

$v \stackrel{\epsilon}{\Longrightarrow} v' \xrightarrow{a} v''$ with $u \equiv v'$ and $u' \equiv v''$.

Thus $vy \stackrel{\epsilon}{\Longrightarrow} v'y \xrightarrow{a} v''y$ with $ux \; R \; v'y$ and $w = u'x \; R \; v''y$.

Hence $ux \; R \; vy$ satisfies condition (i2) of Definition 2.1 .

Case 2: $u = \epsilon$.

Hence $x \xrightarrow{a} w$. As $x \equiv y$, one of the two subcases below applies.

Case 2.1: $a = \epsilon$ and $w \equiv y$.

Then $w = uw \; R \; vy$. Hence $ux \; R \; vy$ satisfies point (i1) of Definition 2.1 .

Case 2.2: there exist y' and y'' such that

$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ with $x \equiv y'$ and $w \equiv y''$.

As $\epsilon \equiv v$ and from (i), $\|v\| = 0$ i.e. $v \stackrel{\epsilon}{\Longrightarrow} \epsilon$.

Thus $vy \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ with $ux \; R \; y'$ and $w \; R \; y''$.

Hence $ux \; R \; vy$ satisfies condition (i2) of Definition 2.1 .

iii) Point (c) follows from the following property:

$uv \stackrel{w}{\Longrightarrow} \epsilon$ iff there exist w', w'' such that $u \stackrel{w'}{\Longrightarrow} \epsilon$ and $v \stackrel{w''}{\Longrightarrow} \epsilon$ with $w'w'' = w$.

□

Lemma 3.8 a) *Every bisimulation is a self-proving relation.*
b) *Every self-proving congruence is a bisimulation.*

Proof.

i) Let R be a bisimulation on a graph G. Let us show that R is self-proving.

Let $p \; R \; q$.

In particular $p \equiv q$ and from Lemma 3.6 (b), $\|p\| = \|q\|$. So $\|p\| = 0$ iff $\|q\| = 0$ hence $p \; R \; q$ satisfies point (i) of Definition 3.7 .

By symmetry of Definition 2.1, it remains to prove point (ii2) of Definition 3.7.

Suppose that $p \stackrel{\epsilon}{\Longrightarrow} p' \xrightarrow{a} p''$. As $p \; R \; q$ and by induction on the length of the derivation $p \stackrel{\epsilon}{\Longrightarrow} p'$, there exists q' such that $q \stackrel{\epsilon}{\Longrightarrow} q'$ and $p' \; R \; q'$.

As $p' \; R \; q'$ and $p' \xrightarrow{a} p''$, one of the two cases below applies.

Case 1: $a = \epsilon$ and $p'' \; R \; q'$.

In particular $p' \underset{R}{\overset{*}{\longleftrightarrow}} q'$ and $p'' \underset{R}{\overset{*}{\longleftrightarrow}} q'$.

Hence point (ii1) of Definition 3.7 is satisfied.

Case 2: there exist r and q'' such that

$q' \stackrel{\epsilon}{\Longrightarrow} r \xrightarrow{a} q''$ with $p' \; R \; r$ and $p'' \; R \; q''$.

Thus $q \stackrel{\epsilon}{\Longrightarrow} r$, $p' \underset{R}{\overset{*}{\longleftrightarrow}} r$ and $p'' \underset{R}{\overset{*}{\longleftrightarrow}} q''$.

Hence point (ii2) of Definition 3.7 is satisfied.

ii) Let R be a self-proving relation which is a congruence, i.e. R is an equivalence such

that $R.R \subseteq R$. Let us show that R is a bisimulation.
As R is a congruence, note that its least congruence closure $\overset{*}{\underset{R}{\longleftrightarrow}}$ is equal to R. As R is symmetrical, it suffices to show that $p\ R\ q$ satisfies (i) of Definition 2.1 . Let $p \xrightarrow{a} p'$. One of the two cases below applies.

Case 1: $a = \epsilon$ and there exists q' such that
$$q \overset{\epsilon}{\Longrightarrow} q' \text{ with } p \overset{*}{\underset{R}{\longleftrightarrow}} q' \overset{*}{\underset{R}{\longleftrightarrow}} p'.$$
So $p'\ R\ q'\ R\ p\ R\ q$, hence $p'\ R\ q$.
Thus $p\ R\ q$ satisfies point (i1) of Definition 2.1.

Case 2: there exist q' and q'' such that
$$q \overset{\epsilon}{\Longrightarrow} q' \xrightarrow{a} q'' \text{ with } p \overset{*}{\underset{R}{\longleftrightarrow}} q' \text{ and } p' \overset{*}{\underset{R}{\longleftrightarrow}} q''.$$
Hence $p\ R\ q'$ and $p'\ R\ q''$.
Thus $p\ R\ q$ satisfies point (i2) of Definition 2.1.

□

Proposition 3.9 *A relation* R *is self-proving if and only if its least congruence* $\overset{*}{\underset{R}{\longleftrightarrow}}$ *is a bisimulation.*

Proof.
i) Let us prove the necessary condition.
Let R be a self-proving relation. From Lemma 3.8 (b), it is sufficient to prove that $\overset{*}{\underset{R}{\longleftrightarrow}}$ is self-proving. As the set of self-proving relations is closed by union (finite or infinite), it suffices to show by induction on $n \geq 0$ that $\overset{n}{\underset{R}{\longleftrightarrow}}$ is self-proving.

n = 0: $\overset{0}{\underset{R}{\longleftrightarrow}}$ is the identity on N^* which is a bisimulation.
From Lemma 3.8 (a), $\overset{0}{\underset{R}{\longleftrightarrow}}$ is self-proving.

n = 1: let $p \underset{R}{\longleftrightarrow} q$.
There exist $(p_0, q_0) \in R \cup R^{-1}$ and non-terminal words s, t such that
$$sp_0t = p \text{ and } sq_0t = q.$$
As $p_0\ R\ q_0$ or $q_0\ R\ p_0$ satisfies (i) of 3.7, we have $\|p_0\| = 0$ iff $\|q_0\| = 0$. From Lemma 3.6 (c), we obtain $\|p\| = 0$ iff $\|q\| = 0$, i.e. $p \underset{R}{\longleftrightarrow} q$ satisfies (i) of Definition 3.7.
Let us show that $p \underset{R}{\longleftrightarrow} q$ satisfies (ii) of 3.7.
Let $p \overset{\epsilon}{\Longrightarrow} p' \xrightarrow{a} p''$. As $p = sp_0t$, we distinguish the three complementary cases below.

Case 1: there exist s', s'' such that $s \overset{\epsilon}{\Longrightarrow}$ s' $\xrightarrow{a}$ s" with $p' = s'p_0t$ and $p'' = s''p_0t$.
Thus $q' = s'q_0t$ and $q'' = s''q_0t$ are suitable for (ii2) in 3.7:
$$q \overset{\epsilon}{\Longrightarrow} q' \xrightarrow{a} q'' \text{ with } p' \underset{R}{\longleftrightarrow} q' \text{ and } p'' \underset{R}{\longleftrightarrow} q''.$$

Case 2: $s \overset{\epsilon}{\Longrightarrow} \epsilon$ and there exist p_0' and p_0'' such that
$$p_0 \overset{\epsilon}{\Longrightarrow} p_0' \xrightarrow{a} p_0'' \text{ with } p' = p_0't \text{ and } p'' = p_0''t.$$
As $p_0\ R\ q_0$ or $q_0\ R\ p_0$, one of the two following subcases applies.

Case 2.1: $a = \epsilon$ and there is q_0' such that $q_0 \overset{\epsilon}{\Longrightarrow} q_0'$ with $p_0' \overset{*}{\underset{R}{\longleftrightarrow}} q_0' \overset{*}{\underset{R}{\longleftrightarrow}} p_0''$.

Thus $q' = q'_0 t$ satisfies point (ii1) of Definition 3.7 : $q = sq_0t \stackrel{\epsilon}{\Longrightarrow} q'_0 t = q'$ with $p' = p'_0 t \stackrel{*}{\underset{R}{\longleftrightarrow}} q'_0 t = q'$ and $p'' = p''_0 t \stackrel{*}{\underset{R}{\longleftrightarrow}} q'_0 t = q'$.

Case 2.2: there are q'_0 and q''_0 such that

$q_0 \stackrel{\epsilon}{\Longrightarrow} q'_0 \stackrel{a}{\longrightarrow} q''_0$ with $p'_0 \stackrel{*}{\underset{R}{\longleftrightarrow}} q'_0$ and $p''_0 \stackrel{*}{\underset{R}{\longleftrightarrow}} q''_0$.

Thus $q' = q'_0 t$ and $q'' = q''_0 t$ suit for (ii2) of Definition 3.7:

$q \stackrel{\epsilon}{\Longrightarrow} q' \stackrel{a}{\longrightarrow} q''$ with $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''$.

Case 3: $s \stackrel{\epsilon}{\Longrightarrow} \epsilon$, $p_0 \stackrel{\epsilon}{\Longrightarrow} \epsilon$ and $t \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$.

As $p_0 \stackrel{\epsilon}{\Longrightarrow} \epsilon$ and $(p_0, q_0) \in R \cup R^{-1}$, we have $q_0 \stackrel{\epsilon}{\Longrightarrow} \epsilon$.

Thus p' and p'' suits for (ii2) of 3.7: $q = sq_0t \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$.

Finally $p \stackrel{}{\underset{R}{\longleftrightarrow}} q$ satisfies (ii) of 3.7, and so (iii) of 3.7 by symmetry of $\stackrel{}{\underset{R}{\longleftrightarrow}}$.

n $\Longrightarrow$ n+1: suppose that $p \stackrel{}{\underset{R}{\longleftrightarrow}} r \stackrel{n}{\underset{R}{\longleftrightarrow}} q$. We have

$p \stackrel{\epsilon}{\Longrightarrow} \epsilon$ iff $r \stackrel{\epsilon}{\Longrightarrow} \epsilon$ from case $n = 1$

iff $q \stackrel{\epsilon}{\Longrightarrow} \epsilon$ by induction hypothesis.

So point (i) of 3.7 is satisfied by $p \stackrel{n+1}{\underset{R}{\longleftrightarrow}} q$.

Let us show that $p \stackrel{n+1}{\underset{R}{\longleftrightarrow}} q$ satisfies point (ii) of 3.7.

Let $p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$. As $\stackrel{}{\underset{R}{\longleftrightarrow}}$ is self-proving, one of the two cases below applies.

Case 1: $a = \epsilon$ and there exists r' such that $r \stackrel{\epsilon}{\Longrightarrow} r'$ with $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} r'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} r'$.

By induction hypothesis, $\stackrel{n}{\underset{R}{\longleftrightarrow}}$ is self-proving.

So, there exists q' such that $q \stackrel{\epsilon}{\Longrightarrow} q'$ and $r' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$.

Thus $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$, hence $p \stackrel{n+1}{\underset{R}{\longleftrightarrow}} q$ satisfies (ii1) of 3.7.

Case 2: there exist r' and r'' such that $r \stackrel{\epsilon}{\Longrightarrow} r' \stackrel{a}{\longrightarrow} r''$ with

$p' \stackrel{*}{\underset{R}{\longleftrightarrow}} r'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} r''$.

By induction hypothesis, $\stackrel{n}{\underset{R}{\longleftrightarrow}}$ is self-proving.

So, one of the subcases below applies.

Case 2.1: $a = \epsilon$ and there exists q' such that

$q \stackrel{\epsilon}{\Longrightarrow} q'$ with $r' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $r'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$.

Thus $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$, hence $p \stackrel{n+1}{\underset{R}{\longleftrightarrow}} q$ satisfies (ii1) of 3.7.

Case 2.2: there exist q' and q'' such that

$q \stackrel{\epsilon}{\Longrightarrow} q' \stackrel{a}{\longrightarrow} q''$ with $r' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $r'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''$.

Thus $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''$, hence $p \stackrel{n+1}{\underset{R}{\longleftrightarrow}} q$ satisfies (ii2) of 3.7.

In all cases, $p \stackrel{n+1}{\underset{R}{\longleftrightarrow}} q$ satisfies (ii) of 3.7, and by symmetry of $\stackrel{n+1}{\underset{R}{\longleftrightarrow}}$, point (iii) of Definition 3.7 is also satisfied.

This ends the induction, hence $\stackrel{*}{\underset{R}{\longleftrightarrow}} = \bigcup\{ \stackrel{n}{\underset{R}{\longleftrightarrow}} \mid n \geq 0 \}$ is self-proving, so is a bisimulation from Lemma 3.8 (b).

ii) Let us prove the sufficient condition.

Let R be a binary relation on N^* such that $\stackrel{*}{\underset{R}{\longleftrightarrow}}$ is a bisimulation. Let us prove that R is self-proving.

Let $p \; R \; q$.

In particular $p \equiv q$ and from Lemma 3.6 (b), $\|p\| = \|q\|$. So $\|p\| = 0$ iff $\|q\| = 0$ hence $p\ R\ q$ satisfies point (i) of Definition 3.7.
Let us prove that point (ii) of Definition 3.7 is satisfied. Let $p \stackrel{\epsilon}{\Longrightarrow} p' \stackrel{a}{\longrightarrow} p''$.
As $p \stackrel{*}{\underset{R}{\longleftrightarrow}} q$ and $\stackrel{*}{\underset{R}{\longleftrightarrow}}$ is a bisimulation, by induction on the derivation length of $p \stackrel{\epsilon}{\Longrightarrow} p'$, there exists q' such that $q \stackrel{\epsilon}{\Longrightarrow} q'$ and $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$.
As $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$ and $p' \stackrel{a}{\longrightarrow} p''$, one of the two cases below applies.

Case 1: $a = \epsilon$ and $p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$.

Hence point (ii1) of Definition 3.7 is satisfied.

Case 2: there exist r and q'' such that

$$q' \stackrel{\epsilon}{\Longrightarrow} r \stackrel{a}{\longrightarrow} q'' \text{ with } p' \stackrel{*}{\underset{R}{\longleftrightarrow}} r \text{ and } p'' \stackrel{*}{\underset{R}{\longleftrightarrow}} q''.$$

As $q \stackrel{\epsilon}{\Longrightarrow} r$, point (ii2) of Definition 3.7 is satisfied.

Thus (ii) of Definition 3.7 is satisfied and also point (iii) by symmetry of $\stackrel{*}{\underset{R}{\longleftrightarrow}}$.
Finally R is self-proving.
□

Lemma 3.11 *If* R *is a basic relation then*

a) R *is finite*

b) *the rewriting relation* $\underset{R}{\longrightarrow}$ *is terminating and confluent;*
thus any word u *reduces along* R *to a unique normal form* u↓R.

Proof.
Let R be a basic system. From (i) and (ii) of Definition 3.10, R is finite and $\underset{R}{\longrightarrow}$ is confluent. From (ii) and (iii) of 3.10, every derivation $\underset{R}{\longrightarrow}^*$ from any non-terminal word u is of length at most $|u|.|R|^{n-1}$ where $|u|$ is the length of u, $|R| = max\{\ |v|\ |\ v \in Im(R)\ \}$ is the maximal length of the words in R, and n is the number $\#N$ of non-terminals. Hence $\underset{R}{\longrightarrow}$ is terminating.
□

Lemma 3.12 *If* su ≡ tv *with* $\|s\| = \|t\|$ *then* s ≡ t *and* u ≡ v.

Proof.
From Lemma 3.6 (b),(c), if $su \equiv tv \ \wedge\ \|s\| = \|t\|$ then $\|u\| = \|v\|$.
Thus, it suffices to show that

$$R = \{\ (s,t)\ |\ \|s\| = \|t\| \ \wedge\ \exists u, v,\ su \equiv tv\ \}$$

is a branching bisimulation.
As R is symmetrical, it suffices to show that $s\ R\ t$ satisfies (i) of Definition 2.1. There exist u and v such that $su \equiv tv$. So $\|u\| = \|v\|$. Let $s \stackrel{a}{\longrightarrow} s'$. Hence $su \stackrel{a}{\longrightarrow} s'u$. As $\equiv$ is a bisimulation, one of the two cases below applies.

Case 1: $a = \epsilon$ and $s'u \equiv tv$.

As $\|u\| = \|v\|$ and from Lemma 3.6 (b),(c), $\|s'\| = \|t\|$.
So $s'\ R\ t$ hence (i1) of Definition 2.1 is satisfied.

Case 2: there exist w and w' such that

$$tv \stackrel{\epsilon}{\Longrightarrow} w \stackrel{a}{\longrightarrow} w' \text{ with } su \equiv w \text{ and } s'u \equiv w'.$$

As $s \neq \epsilon$ and P is proper, $\|s\| \neq 0$.
From Lemma 3.6 (b), $su \not\equiv v$.
From Lemma 2.2, there exists $t' \neq \epsilon$ such that $t \stackrel{\epsilon}{\Longrightarrow} t'$ and $w = t'v$.
As $t' \neq \epsilon$, there exists t'' such that

$$t' \stackrel{a}{\longrightarrow} t'' \text{ and } w' = t''v.$$

As $su \equiv t'v$ and $s'u \equiv t''v$ with $\|u\| = \|v\|$, we obtain $s \; R \; t'$ and $s' \; R \; t''$.
Hence point (i2) of Definition 2.1 is satisfied.

□

Lemma 3.13 *If* su ≡ tv *with* ||s|| ≥ ||t|| *then* s ≡ tw *and* wu ≡ v *for some* w.

Proof.
By induction on $n \geq 0$, let us prove the following property (1):

$$su \equiv tv \wedge \|s\| \geq \|t\| \wedge < t >= n \implies \exists w,\ s \equiv tw\ . \tag{1}$$

where $< t >$ is the minimal length of the paths from t to ϵ.
If $< t >= 0$ then $t = \epsilon$ hence $w = s$ suits.
Suppose (1) true for $n \geq 0$ and let $su \equiv tv$, $\|s\| \geq \|t\|$ and $< t >= n + 1$.
From Lemma 3.6 (b),(c), $\|u\| \leq \|v\|$.
As $t \neq \epsilon$ and P is proper, $\|t\| \neq 0$; hence $\|s\| \neq 0$.
There exist a non-terminal word t' and a label a such that $t \stackrel{a}{\longrightarrow} t'$ and $< t' >= n$.
Thus $su \equiv tv \stackrel{a}{\longrightarrow} t'v$ and one of the two cases below applies.
Case 1: $a = \epsilon$ and $su \equiv t'v$.
So $tv \equiv t'v$ and from Lemma 3.12, $t \equiv t'$.
So $\|s\| \geq \|t\| = \|t'\|$ and by induction hypothesis,
there exists w such that $s \equiv t'w$. Hence $s \equiv tw$.
Case 2: there exist w' and w'' such that

$$su \stackrel{\epsilon}{\Longrightarrow} w' \stackrel{a}{\longrightarrow} w'' \text{ with } w' \equiv tv \text{ and } w'' \equiv t'v.$$

As $\|s\| \neq 0$ and from Lemma 3.6 (b), $u \not\equiv tv$.
From Lemma 2.2, there exists $s' \neq \epsilon$ such that $s \stackrel{\epsilon}{\Longrightarrow} s'$ and $w' = s'u$.
So there exists s'' such that $s' \stackrel{a}{\longrightarrow} s''$ and $s''u = w''$.
Hence $s''u \equiv t'v$. As $\|u\| \leq \|v\|$, we have $\|s''\| \geq \|t'\|$.
By induction hypothesis, there exists w such that $s'' \equiv t'w$.
Thus $t'wu \equiv t'v$ and from Lemma 3.12, $wu \equiv v$.
So $su \equiv tv \equiv twu$ and from Lemma 3.12, $s \equiv tw$.
This ends the induction, and there exists w such that $s \equiv tw$.
Consequently $twu \equiv su \equiv tv$ and from Lemma 3.12, $wu \equiv v$.
□

Theorem 3.14 *Among the basic and self-proving relations, those that are maximal for inclusion generates the branching bisimulation* $\equiv$.

Proof.
Note that the empty relation is basic, self-proving and included in $\equiv$. Furthermore, the set of basic relations is finite.
i) Let R be a basic relation $\subseteq \equiv$ which is maximal for inclusion. Let us show that R generates $\equiv$, i.e. $\xleftrightarrow[R]{*} = \equiv$.
As $R \subseteq \equiv$ and $\equiv$ is a congruence, we have $\xleftrightarrow[R]{*} \subseteq \equiv$.
Conversely, let $u \equiv v$. From Lemma 3.11, the normal forms $u{\downarrow}R$ and $v{\downarrow}R$ of u and v exist.
As $\xleftrightarrow[R]{*} \subseteq \equiv$, we have $u{\downarrow}R \equiv v{\downarrow}R$. From Lemma 3.6 (b), $\|u{\downarrow}R\| = \|v{\downarrow}R\|$.
Suppose that $u{\downarrow}R \neq v{\downarrow}R$.
As P is proper and reduced, and $u{\downarrow}R$ has the same norm as $v{\downarrow}R$, the word $u{\downarrow}R$ (resp. $v{\downarrow}R$) is not a prefix of $v{\downarrow}R$ (resp. $u{\downarrow}R$). So, there exist non-terminal words w, x, y, u', v' such that

$$u{\downarrow}R = wxu' \text{ and } v{\downarrow}R = wyv' \text{ with } x, y \in N \text{ and } x \neq y.$$

From Lemma 3.12, $xu' \equiv yv'$. From Lemma 3.13, there exists a non-terminal word z such that

$$x \equiv yz \text{ or } y \equiv xz.$$

So $x \equiv y(z{\downarrow}R)$ or $y \equiv x(z{\downarrow}R)$ which is a contradiction with the maximality of R.
Therefore $u{\downarrow}R = v{\downarrow}R$ hence $u \xleftrightarrow[R]{*} v$. Finally $\equiv \; = \xleftrightarrow[R]{*}$.

ii) There exists a basic and self-proving relation R which is maximal for inclusion. From Proposition 3.9, $\xleftrightarrow[R]{*}$ is a bisimulation. In particular $R \subseteq \equiv$.
So, we can consider a basic relation $S \supseteq R$, included in $\equiv$ and which is maximal for inclusion. From point (i), $\xleftrightarrow[S]{*} = \equiv$.
From Proposition 3.9, S is self-proving and by maximality of R, we have $S = R$, hence $\xleftrightarrow[R]{*} = \equiv$.
□

Corollary 3.15 u $\equiv$ v *iff* u$\downarrow$R = v$\downarrow$R *for some basic and self-proving relation* R.

Proof.
i) Let us prove the "only if" part. Let $u \equiv v$. From Theorem 3.14, there exists a basic and self-proving relation R such that $u \xleftrightarrow[R]{*} v$. From Lemma 3.11 (b), R is canonical, so $u{\downarrow}R = v{\downarrow}R$.
ii) Let us prove the "if" part. Let R be a basic and self-proving relation such that $u{\downarrow}R = v{\downarrow}R$. In particular $u \xleftrightarrow[R]{*} v$ and from Proposition 3.9, $u \equiv v$.
□

Lemma 3.16 *A basic relation* R *is self-proving (w.r.t.* P*) if and only if for all* $y \in N$ *and for all* $(x \xrightarrow{a} x') \in P$ *with* $(a \neq \epsilon$ *or* $x{\downarrow}R \neq x'{\downarrow}R)$*, the two following conditions are satisfied:*

(i) if $x{\downarrow}R \leq y{\downarrow}R$ *then there exist* y', y'' *such that*
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ *with* $y{\downarrow}R = y'{\downarrow}R$ *and* $(y{\downarrow}R)/(x{\downarrow}R) = (y''{\downarrow}R)/(x'{\downarrow}R)$

(ii) if $x{\downarrow}R > y{\downarrow}R$ *then there exist* y', y'' *such that*
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ *with* $y{\downarrow}R = y'{\downarrow}R$ *and* $(x{\downarrow}R)/(y{\downarrow}R) = (x'{\downarrow}R)/(y''{\downarrow}R)$.

Proof.

i) Let R be a basic and self-proving relation. Let $y \in N$ and let $(x \xrightarrow{a} x') \in P$ with $a \neq \epsilon$ or $x{\downarrow}R \neq x'{\downarrow}R$.

From Proposition 3.9, $\stackrel{*}{\underset{R}{\longleftrightarrow}}$ is a bisimulation.

a) Let us show that R satisfies point (i) of 3.16. Suppose there exists u such that $(x{\downarrow}R)u = y{\downarrow}R$. In particular $u{\downarrow}R = u$. Furthermore $xu \stackrel{*}{\underset{R}{\longleftrightarrow}} y$. As $\stackrel{*}{\underset{R}{\longleftrightarrow}}$ is a bisimulation, we have one of the two cases below.

Case 1: $a = \epsilon$ and $x'u \stackrel{*}{\underset{R}{\longleftrightarrow}} y$.

So $x{\downarrow}R = x'{\downarrow}R$ which is forbidden.

Case 2: there exist y' and y'' such that
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ with $xu \stackrel{*}{\underset{R}{\longleftrightarrow}} y'$ and $x'u \stackrel{*}{\underset{R}{\longleftrightarrow}} y''$.

So $y \stackrel{*}{\underset{R}{\longleftrightarrow}} y'$ i.e $y{\downarrow}R = y'{\downarrow}R$. Furthermore $(x'{\downarrow}R)u = (x'u){\downarrow}R = y''{\downarrow}R$.

Thus (i) of 3.16 is satisfied.

b) Let us show that R satisfies point (ii) of 3.16. Suppose there exists u such that $x{\downarrow}R = (y{\downarrow}R)u$. We have one of the two cases below.

Case 1: $a = \epsilon$ and $x' \stackrel{*}{\underset{R}{\longleftrightarrow}} yu$.

So $x{\downarrow}R = x'{\downarrow}R$ which is forbidden.

Case 2: there exist u' and u'' such that
$yu \stackrel{\epsilon}{\Longrightarrow} u' \xrightarrow{a} u''$ with $x \stackrel{*}{\underset{R}{\longleftrightarrow}} u'$ and $x' \stackrel{*}{\underset{R}{\longleftrightarrow}} u''$.

As P is proper, there exists $y' \neq \epsilon$ such that $y \stackrel{\epsilon}{\Longrightarrow} y'$ and $u' = y'u$.

So, there exists y'' such that $y' \xrightarrow{a} y''$ and $u'' = y''u$.

As $yu \stackrel{*}{\underset{R}{\longleftrightarrow}} x \stackrel{*}{\underset{R}{\longleftrightarrow}} u' = y'u$, we have $y{\downarrow}R = y'{\downarrow}R$.

Furthermore $y''u = u'' \stackrel{*}{\underset{R}{\longleftrightarrow}} x'$ i.e. $x'{\downarrow}R = (y''u){\downarrow}R = (y''{\downarrow}R)u$.

Finally, the necessary condition of this lemma is proved.

ii) Let R be a basic relation satisfying conditions (i) and (ii) of this lemma. Let us show that R is self-proving.

a) Let us show that pRq and $p \stackrel{\epsilon}{\Longrightarrow} p'$ implies there exists q' such that
$q \stackrel{\epsilon}{\Longrightarrow} q'$ and $p' \stackrel{*}{\underset{R}{\longleftrightarrow}} q'$.

By induction on the length of the derivation $\stackrel{\epsilon}{\Longrightarrow}$, it is sufficient to prove the following property:

if $p \xleftarrow[R]{*} q$ and $p \xrightarrow{\epsilon} p'$ then there exists q' such that $q \stackrel{\epsilon}{\Longrightarrow} q'$ and $p' \xleftarrow[R]{*} q'$.

Suppose that $p \xleftarrow[R]{*} q$ and $p \xrightarrow{\epsilon} p'$. In particular $p \neq \epsilon$. As R is basic and $p \xleftarrow[R]{*} q$, we have also $q \neq \epsilon$. So, there exist $x, y \in N$ and $s, t \in N^*$ such that $p = xs$ and $q = yt$. It follows that

$$(x\downarrow R)(s\downarrow R) = (y\downarrow R)(t\downarrow R).$$

There exists x' such that $x \xrightarrow{\epsilon} x'$ and $p' = x's$. We consider the three following cases:

Case 1: $x\downarrow R = x'\downarrow R$. Then $q \xleftarrow[R]{*} p'$ hence $q' = q$ suits.

Case 2: $x\downarrow R \neq x'\downarrow R$ and $x\downarrow R \leq y\downarrow R$. Then there exists u such that $(x\downarrow R)u = y\downarrow R$. So $s\downarrow R = u(t\downarrow R)$.

From (i) of this lemma, there exist y' and y'' such that
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{\epsilon} y''$ with $y\downarrow R = y'\downarrow R$ and $y''\downarrow R = (x'\downarrow R)u$.

Hence $q' = y''t$ suits because $y''t \xleftarrow[R]{*} x'ut \xleftarrow[R]{*} x's = p'$.

Case 3: $x\downarrow R \neq x'\downarrow R$ and $x\downarrow R > y\downarrow R$. Then there exists u such that $x\downarrow R = (y\downarrow R)u$. So $u(s\downarrow R) = t\downarrow R$.

From (ii) of this lemma, there exist y' and y'' such that
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{\epsilon} y''$ with $y\downarrow R = y'\downarrow R$ and $x'\downarrow R = (y''\downarrow R)u$.

Hence $q' = y''t$ suits because $y''t \xleftarrow[R]{*} y''us \xleftarrow[R]{*} x's = p'$.

b) Let us show that $p\ R\ q$ satisfies (i) of Definition 3.7. As R is basic, $p \neq \epsilon$. As P is proper, we have not $p \stackrel{\epsilon}{\Longrightarrow} \epsilon$. So condition (i) of 3.7 is always satisfied.

c) Let us show that $p\ R\ q$ satisfies (ii) of Definition 3.7.

Suppose that $p \stackrel{\epsilon}{\Longrightarrow} p' \xrightarrow{a} p''$.

From point (a), there exists q' such that $q \stackrel{\epsilon}{\Longrightarrow} q'$ and $p'\downarrow R = q'\downarrow R$.

As $p' \xrightarrow{a} p''$, there exists a rule $x \xrightarrow{a} x'$ of P and a non-terminal word s such that
$p' = xs$ and $p'' = x's$.

We distinguish the two cases below.

Case 1: $a = \epsilon$ and $x\downarrow R = x'\downarrow R$.

So $p''\downarrow R = p'\downarrow R = q'\downarrow R$, hence point (ii1) of 3.7 is satisfied.

Case 2: $a \neq \epsilon$ or $x\downarrow R \neq x'\downarrow R$.

As $(xs)\downarrow R = q'\downarrow R$ and R is ϵ-free, $q' \neq \epsilon$.

So there exist $y \in N$ and t such that $q' = yt$.

As R is alphabetic, we have
$(x\downarrow R)(s\downarrow R) = (y\downarrow R)(t\downarrow R)$.

One of the two subcases below applies.

Case 2.1: $|x\downarrow R| \leq |y\downarrow R|$.

So there exists u such that $(x\downarrow R)u = y\downarrow R$.

Hence $u\downarrow R = u$. So $(xu)\downarrow R = y\downarrow R$ and $s\downarrow R = (ut)\downarrow R$.

From (i) of this lemma, there exist y' and y'' such that
$y \stackrel{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ with $y\downarrow R = y'\downarrow R$ and $(x'\downarrow R)u = y''\downarrow R$.

Thus $q \stackrel{\epsilon}{\Longrightarrow} y't \xrightarrow{a} y''t$ with
$p' = xs \xleftarrow[R]{*} xut \xleftarrow[R]{*} yt \xleftarrow[R]{*} y't$ .and
$p'' = x's \xleftarrow[R]{*} x'ut \xleftarrow[R]{*} y''t$.

Hence point (ii2) of Definition 3.7 is satisfied.

Case 2.2: $|x\downarrow R| > |y\downarrow R|$.

So there exists u such that $x\downarrow R = (y\downarrow R)u$.

Hence $u{\downarrow}R = u$. So $x{\downarrow}R = (yu){\downarrow}R$ and $(us){\downarrow}R = t{\downarrow}R$.
From (ii) of this lemma, there exist y' and y'' such that
$y \stackrel{\epsilon}{\Longrightarrow} y' \stackrel{a}{\longrightarrow} y''$ with $y{\downarrow}R = y'{\downarrow}R$ and $x'{\downarrow}R = (y''u){\downarrow}R$.
Thus $q \stackrel{\epsilon}{\Longrightarrow} y't \stackrel{a}{\longrightarrow} y''t$ with

$p' = xs \stackrel{*}{\underset{R}{\longleftrightarrow}} yus \stackrel{*}{\underset{R}{\longleftrightarrow}} yt \stackrel{*}{\underset{R}{\longleftrightarrow}} y't$ and

$p'' = x's \stackrel{*}{\underset{R}{\longleftrightarrow}} y''us \stackrel{*}{\underset{R}{\longleftrightarrow}} y''t.$

Hence point (ii2) of Definition 3.7 is satisfied.
In a symmetrical way, R satisfies point (iii) of Definition 3.7. Finally R is self-proving.
□

Proposition 3.17 *One may decide whether a basic relation is self-proving.*

Proof.
Let R be a basic relation.
First, we test whether R is norm-preserving. From Proposition 3.9 and Lemma 3.6 (b), if R is not norm preserving then R is not self-proving. Now, suppose that R is norm-preserving and let y be a non-terminal (letter). From Proposition 3.16, to decide whether R is self-proving, it is sufficient to be able to construct the following finite set A:

$$A = \{\, y' \mid y \stackrel{\epsilon}{\Longrightarrow} y' \wedge y{\downarrow}R = y'{\downarrow}R \,\}.$$

In fact P being proper, this set A is finite because the maximal length of its words y' is finite:

$$|y'| \leq \|y'\| = \|y'{\downarrow}R\| = \|y{\downarrow}R\|.$$

Generally speaking, the relation $\stackrel{\epsilon}{\Longrightarrow}$ is equal to the prefix derivation $\stackrel{*}{\underset{Q}{\longmapsto}}$ according to the system

$$Q = \{\, (x,u) \mid (x \stackrel{\epsilon}{\longrightarrow} u) \in P \,\}$$

of the ϵ-rules of P. From [Bü 64], we can construct a finite automaton recognizing the rational language

$$\{\, y' \mid y \stackrel{*}{\underset{Q}{\longmapsto}} y' \,\} = \{\, y' \mid y \stackrel{\epsilon}{\Longrightarrow} y' \,\}$$

of words which are accessible from y by ϵ-transitions. So, we can construct the finite set

$$\{\, y' \mid y \stackrel{\epsilon}{\Longrightarrow} y' \wedge |y'| \leq \|y{\downarrow}R\| \,\}$$

and its subset A.
□

Theorem 3.19 *Given a proper and reduced alphabetic system* P *and an axiom* p, *one can effectively construct a proper and reduced alphabetic system* Q *and an axiom* q *such that:*

a) *the context-free process* $_q\stackrel{}{\underset{Q}{\longmapsto}}$ *is isomorphic to the quotient of the context-free process* $_p\stackrel{}{\underset{P}{\longmapsto}}$ *by its greatest branching bisimulation,*

b) *the union of all the cf-processes of* Q *is isomorphic to the quotient of the union of all the cf-processes of* P *by its greatest branching bisimulation.*

Proof.

Let P be a reduced and proper alphabetic system. Let p be a non-terminal word. From Theorem 3.14 and Proposition 3.17, we extract a basic relation R such that $\overset{*}{\underset{R}{\longleftrightarrow}} = \equiv$. Then, we construct the following reduced and proper alphabetic system

$$Q = \{ x\downarrow R \xrightarrow{a} u\downarrow R \mid (x \xrightarrow{a} u) \in P \wedge |x\downarrow R| = 1 \wedge (x\downarrow R = u\downarrow R \Longrightarrow a \neq \epsilon) \} .$$

where its set of non-terminals is restricted to the set of irreducible non-terminals of P. Given a graph G with vertices in N^*, we define

$$G\downarrow R = \{ u\downarrow R \xrightarrow{a} v\downarrow R \mid (u \xrightarrow{a} v) \in G \wedge (u\downarrow R = v\downarrow R \Longrightarrow a \neq \epsilon) \}.$$

So $G\downarrow R$ is isomorphic to $G/\equiv$. To show this theorem, it suffices to prove the following equalities:

$$_{p\downarrow R}\!\!\underset{Q}{\longmapsto} = (_{p}\!\!\underset{P}{\longmapsto})\downarrow R \text{ and } \underset{Q}{\overset{a}{\longmapsto}} = (\underset{P}{\overset{a}{\longmapsto}})\downarrow R \text{ for every label } a.$$

i) Let us show that $_{p\downarrow R}\!\!\underset{Q}{\longmapsto} \subseteq (_{p}\!\!\underset{P}{\longmapsto})\downarrow R$ and $\underset{Q}{\overset{a}{\longmapsto}} \subseteq (\underset{P}{\overset{a}{\longmapsto}})\downarrow R$.

As every non-terminal of Q is an irrreducible non-terminal of P, it suffices to prove that

$$u\downarrow R \underset{Q}{\overset{a}{\longmapsto}} v' \Longrightarrow \exists u', v,\ u \overset{\epsilon}{\underset{P}{\Longrightarrow}} u' \underset{P}{\overset{a}{\longmapsto}} v \wedge u\downarrow R = u'\downarrow R \wedge v\downarrow R = v' \wedge (u'\downarrow R = v\downarrow R \Rightarrow a \neq \epsilon).$$

Suppose that $u\downarrow R \underset{Q}{\overset{a}{\longmapsto}} v'$. So $u\downarrow R \neq \epsilon$ and we write $u\downarrow R = yw$ where y is a letter. In particular, y and w are irreducible. By definition of Q, there exists a rule $x \xrightarrow{a} x'$ of P such that $x\downarrow R = y$ and $(x\downarrow R = x'\downarrow R \Rightarrow a \neq \epsilon)$ and $v' = (x'\downarrow R)w$.
Thus $(xw)\downarrow R = yw = u\downarrow R$ and $(x'w)\downarrow R = v'$.
Consequently, $xw \equiv u$ and $xw \underset{P}{\overset{a}{\longmapsto}} x'w$.
As $\equiv$ is a bisimulation, one of the two cases below applies.

Case 1: $a = \epsilon$ and $x'w \equiv u$.
Therefore $xw \equiv x'w$ and from Lemma 3.12, $x \equiv x'$.
Thus $x \overset{*}{\underset{R}{\longleftrightarrow}} x'$ i.e. $x\downarrow R = x'\downarrow R$ which is forbidden for $a = \epsilon$.

Case 2: there exist u' and v such that $u \overset{\epsilon}{\Longrightarrow} u' \xrightarrow{a} v$ according to P with $xw \equiv u'$ and $x'w \equiv v$.
Thus $u\downarrow R = (xw)\downarrow R = u'\downarrow R$ and $v\downarrow R = (x'w)\downarrow R = v'$.
Furthermore, if $u'\downarrow R = v\downarrow R$ then $(xw)\downarrow R = (x'w)\downarrow R$.
Hence $x\downarrow R = x'\downarrow R$ which implies that $a \neq \epsilon$.

ii) Let us show that $(_{p}\!\!\underset{P}{\longmapsto})\downarrow R \subseteq _{p\downarrow R}\!\!\underset{Q}{\longmapsto}$ and $(\underset{P}{\overset{a}{\longmapsto}})\downarrow R \subseteq \underset{Q}{\overset{a}{\longmapsto}}$.

It suffices to show that

$$u \underset{P}{\overset{a}{\longmapsto}} v \Longrightarrow u\downarrow R \underset{Q}{\overset{a}{\longmapsto}} v\downarrow R \vee (u\downarrow R = v\downarrow R \wedge a = \epsilon).$$

Let $u \underset{P}{\overset{a}{\longmapsto}} v$. There exist a rule $x \xrightarrow{a} x'$ of P and a non-terminal word w such that $u = xw$ and $v = x'w$. Write $x\downarrow R = yz$ with $y \in N$. From Proposition 3.9, R is self-proving. We consider the two cases below.

Case 1: $a = \epsilon \wedge x\downarrow R = x'\downarrow R$. Hence $u\downarrow R = v\downarrow R$.

Case 2: $a \neq \epsilon \vee x\downarrow R \neq x'\downarrow R$.
From Lemma 3.16 (ii), there exist y' and y'' such that
$y \overset{\epsilon}{\Longrightarrow} y' \xrightarrow{a} y''$ with $y\downarrow R = y'\downarrow R$ and $x'\downarrow R = (y''z)\downarrow R$.

Thus $y'\downarrow R = y \in N$ so $y' \in N$.
if $y'\downarrow R = y''\downarrow R$ then $x\downarrow R = x'\downarrow R$ hence $a \neq \epsilon$.
Hence $y'\downarrow R \xrightarrow{a} y''\downarrow R$ is a rule of Q. Consequently

$$x\downarrow R = yz = (y'\downarrow R)z \xmapsto[Q]{a} (y''\downarrow R)z = (y''z)\downarrow R = x'\downarrow R.$$

Thus $u\downarrow R = (x\downarrow R)(w\downarrow R) \xmapsto[Q]{a} (x'\downarrow R)(w\downarrow R) = v\downarrow R.$

□

Lemma 4.1 *If* $u \Downarrow v$ *then* $|v| \leq |u| + (n-1)(m-1)$.

Proof.
Consider a norm-non-increasing path $u = u_0 \xmapsto[P]{} u_1 \ \ldots \xmapsto[P]{} u_k = v$, that is $\|u_{i+1}\| \leq \|u_i\|$ for every $0 \leq i < k$.
We define a maximal decreasing integer sequence $k = k(0) > k(1) > \ldots > k(l)$ such that for every $0 \leq i < l$, we have

$$|u_{k(i)}| > |u|$$
$$\text{and} \quad k(i+1) = max\{\, j < k(i) \mid |u_j| < |u_{k(i)}| \,\}.$$

By maximality of l, $|u_{k(l)}| \leq |u|$.
For every $0 \leq i < l$ and by definition of $k(i+1)$, there exist $x \in N$ and $y, z \in N^*$ such that

$$u_{k(i+1)} = xz \ , u_{k(i)} = yz \text{ with } 2 \leq |y| \leq m \text{ and } \|y\| \leq \|x\|.$$

By induction on j with $0 \leq i < j \leq l$, there exist $x \in N$ and $y, z \in N^*$ such that

$$u_{k(j)} = xz \ , u_{k(i)} = yz \text{ with } 2 \leq |y| \leq (j-i)(m-1)+1 \text{ and } \|y\| \leq \|x\|.$$

As $|y| \geq 2$ and $\|y\| \leq \|x\|$, the first letter $y(1)$ of y is different from x, that is $u_{k(i)}(1) \neq u_{k(j)}(1)$ for any $0 \leq i < j \leq l$. Consequently $l \leq n-1$.
If $l = 0$ then $|v| = |u_k| = |u_{k(l)}| \leq |u|$ and the inequality is satisfied.
If $l \neq 0$, there exist $x \in N$ and $y, z \in N^*$ such that

$$u_{k(l)} = xz \text{ and } u_{k(0)} = yz \text{ with } |y| \leq l(m-1)+1 \ .$$

Thus $|v| - |u| = |u_{k(0)}| - |u| \leq |u_{k(0)}| - |u_{k(l)}| = |y| - 1 \leq (n-1)(m-1)$.
□

We denote by $u \Downarrow_w v$ if there exists a norm-non-increasing path $u \Downarrow v$ from u to v labeled by w.

Lemma 4.3 *Given a bisimulation* R *and* $x \ R \ yu$ *with* $x, y \in N$, $u \in N^*$, *there exists* v *such that* $v \ R \ u$ *and* $|v| \leq (n-1)(m-1)+1$.

Proof.
Let R be a bisimulation. From Lemma 3.6 (b), R is norm-preserving. By induction on $\|w\| \geq 0$, if $u \ R \ v$ and $v \Downarrow_w v'$, there exists u' such that $u \Downarrow_w u'$ and $u' \ R \ v'$.
Let $x, y \in N$ and $u \in N^*$ such that $x \ R \ yu$. As P is reduced, there exists w such that $y \Downarrow_w \epsilon$ and $|w| = \|y\|$. Thus $yu \Downarrow_w u$. So, there exists v such that $x \Downarrow_w v$ and $v \ R \ u$.

From Lemma 4.1, $|v| \leq 1 + (n-1)(m-1)$.
□

Proposition 4.4 *There exists a basic self-proving relation R, maximal w.r.t. inclusion of length $|R| \leq (n-1)(m-1)+2$.*

Proof.
Consider the following total order $<$ on N^*:

$$u < v \quad \text{if} \quad (|u| < |v|) \vee (|u| = |v| \wedge u <_{lex} v)$$

where $<_{lex}$ is the lexicographic order. Let us define the following relation

$$R = \{ (x,u) \mid x \in N \wedge x \equiv u \wedge x < u \wedge \forall v \, (x \equiv v \wedge x < v \Rightarrow u \leq v) \}$$

associating to every non-terminal x having a non empty set $A(x) = \{ u \mid x \equiv u \wedge x < u \}$, the minimal element of $A(x)$ w.r.t. $<$. From Lemma 4.3, $|R| \leq (n-1)(m-1)+2$.

i) Let us show that R is basic.

By definition of R, R is alphabetic and functional. As R is included in $\equiv$ and by Lemma 3.6 (b), R is norm-preserving. As R is included in $<$, R has no cycle, i.e. the transitive closure R^+ of R w.r.t. composition is irreflexive. It follows that R is eventually irreducible. Thus R is basic.

ii) Let us show that $u{\downarrow}R = max_{\leq}\{ v \mid u \equiv v \}$ for every non-terminal word u.

As $u \equiv u{\downarrow}R$, it suffices to show by induction on $\|u\| \geq 0$ that

$$\forall v \, (v \equiv u{\downarrow}R \wedge v \neq u{\downarrow}R \implies v < u{\downarrow}R) .$$

$\|u\| = 0$: $u = \epsilon$. As P is reduced and proper, ϵ is the unique word equivalent to itself.
So the basic step of the induction is satisfied.

$\|u\| \neq 0$: let $v \neq u{\downarrow}R$ with $v \equiv u{\downarrow}R$.
From Lemma 3.6 (b), $\|v\| = \|u{\downarrow}R\| = \|u\| > 0$. So, there exist $x, y \in N$ with $x \neq y$, and $u', v', w \in N^*$ such that

$$u{\downarrow}R = wxu' \quad \text{and} \quad v = wyv' .$$

From Lemma 3.12, $xu' \equiv yv'$.
As $x{\downarrow}R = x$, we have $x \notin Dom(R)$. By definition of R and from Lemma 3.13, we obtain

$$\|x\| < \|y\| \quad \vee \quad (\|x\| = \|y\| \wedge y < x).$$

In particular $\|x\| \leq \|y\|$ and by Lemma 3.13, there exists $z \in N^*$ such that

$$xz \equiv y \quad \text{and} \quad u' \equiv zv' .$$

It follows that $y < xz$.
As $\|u'\| < \|xu'\| \leq \|u{\downarrow}R\| = \|u\|$ and $u'{\downarrow}R = u'$, we have by induction hypothesis that $zv' \leq u'$.
Finally $v = wyv' < wxzv' \leq wxu' = u{\downarrow}R$.

This completes the induction and hence the proof of (ii).

iii) Let us show that R is self-proving.

From (ii), if $u \equiv v$ then $u{\downarrow}R = v{\downarrow}R$. So $\equiv$ is included in $\overset{*}{\underset{R}{\longleftrightarrow}}$.

Conversely $R \subseteq \equiv$, hence the greatest bisimulation $\equiv$ is equal to $\overset{*}{\underset{R}{\longleftrightarrow}}$.

Finally R is self-proving by Proposition 3.9.

iv) Let us show that R is a maximal basic and self-proving relation.

Consider a basic and self-proving relation $S \supseteq R$. Let $x\ S\ u$. From Lemma 3.8 (b), we have $x \equiv u \equiv u{\downarrow}R$. We distinguish the three complementary cases below.

Case 1: $x < u{\downarrow}R$. Then $x \in Dom(R)$.

Case 2: $x = u{\downarrow}R$. As $R \subseteq S$, $x \xrightarrow[S]{}{}^{+} u{\downarrow}R = x$ which is in contradiction with the fact that S is basic.

Case 3: $u{\downarrow}R < x$. So $u{\downarrow}R \in Dom(R)$ which is a contradiction.

Finally $Dom(S) = Dom(R)$ hence $S = R$.

□

Lemma 4.6 *Given a functional relation R in $N \times N^+$, the problem of deciding whether R is basic is in* P.

Proof.

Let $M = \{\ u(i) \mid\ u \in Dom(P) \cup Im(P)\ \wedge\ 1 \leq i \leq |u|\ \}$ be the set of non-terminals in P. Consider the following sequence:

$$N_1 = M - Dom(R)$$

and $N_{i+1} = N_i \cup \{\ x \mid \exists u \in N_i^+,\ x\ R\ u\ \}$ for every $i \geq 1$.

As $Dom(P)$ is finite, the integer $p = min\{\ i \mid N_i = N_{i+1}\ \}$ exists and $p \leq n$. Furthermore R is basic iff $N_p = M$.

□

Lemma 4.7 *Given a basic relation R and non-terminal words x, y, u, v, the problem of deciding whether $(x{\downarrow}R)/(y{\downarrow}R) \leq (u{\downarrow}R)/(v{\downarrow}R)$ is in* co-NP.

Proof.

Let R be a basic relation and M be the set of non-terminals in P. For every $x \in Dom(R)$, we denote by r_x its associated right hand side in R, i.e. $x\ R\ r_x$. Otherwise $r_x = x$ for every $x \in M - Dom(R)$.

i) Given a non-terminal word u, let us show that the length $|u{\downarrow}R|$ of its normal form is computable in polynomial time.

Note that a non-terminal x may have a normal form $x{\downarrow}R$ of exponential length.

We determine a sequence $l_0, \ldots, l_{n-1}$ of functions from M into the set of integers, and defined inductively as follows:

$$l_0(x) = 1 \qquad \text{for every } x \in M$$

and $l_{i+1}(x) = \sum_{j=1}^{|r_x|} l_i(r_x(j))$ for every $x \in M$ and $0 \leq i < n-1$.

Then $|x{\downarrow}R| = l_{n-1}(x)$ for every $x \in M$. So $|u{\downarrow}R| = \sum_{j=1}^{|u|} l_{n-1}(u(j))$ is computable in polynomial time.

ii) Given a non-terminal word u and $1 \leq i \leq |u|$, let us show that the i^{th} letter $u{\downarrow}R(i)$ of $u{\downarrow}R$ is computable in polynomial time.

We denote by $u\backslash j = u(1)\ldots u(j)$ the prefix of u of length $0 \leq j \leq |u|$; in particular $u\backslash 0 = \epsilon$. We compute $u{\downarrow}R(i)$ by the procedure below.

While $i \neq 1$ or $u(1) \in Dom(R)$

let $j \geq 0$ be such that $|(u\backslash j)\downarrow R| < i \leq |(u\backslash(j+1))\downarrow R|$
$u := r_{u(j+1)}$
$i := i - |(u\backslash j)\downarrow R|$
endwhile
return $u(1)$

Since R is basic, we have at most n repetitions. From (i), it follows that this algorithm runs in polynomial time.

iii) Let $x, y, u, v \in N^*$. The inequality $(x\downarrow R)/(y\downarrow R) \leq (u\downarrow R)/(v\downarrow R)$ means that

$$\begin{array}{rcll} |y\downarrow R| & \leq & |x\downarrow R| & \wedge \quad x\downarrow R(i) = y\downarrow R(i),\ 1 \leq i \leq |y\downarrow R| \\ |v\downarrow R| & \leq & |u\downarrow R| & \wedge \quad u\downarrow R(i) = v\downarrow R(i),\ 1 \leq i \leq |v\downarrow R| \\ |x\downarrow R| + |v\downarrow R| & \leq & |y\downarrow R| + |u\downarrow R| & \wedge \quad x\downarrow R(|y\downarrow R| + i) = u\downarrow R(|v\downarrow R| + i) \\ & & & \qquad \text{for all } 1 \leq i \leq |x\downarrow R| - |y\downarrow R|. \end{array}$$

From (i) and (ii), this can be done in co-NP.
□

Proposition 4.8 *The problem of deciding whether a basic relation is self-proving is in* Σ_2^p.

Proof.
Let R be a basic relation. We decide whether R is self-proving by applying Lemma 3.16 with Corollary 4.2.

For all $y \in M$ and production $x \xrightarrow{a} x'$,

either	$a = \epsilon$ and $x\downarrow R = x'\downarrow R$	(co-NP)
or	$\neg(x\downarrow R \leq y\downarrow R) \wedge \neg(x\downarrow R > y\downarrow R)$	(NP)
or	existentially choose y' and y'' with	
	$\lvert y'\rvert \leq (n-1)(m-1)+1$ and $\lvert y''\rvert \leq n(m-1)+1$	(NP)
	i) verify that $y \stackrel{\epsilon}{\Longrightarrow} y'$ and $y' \xrightarrow{a} y''$	(P)
	ii) verify that $y\downarrow R = y'\downarrow R$	(co-NP)
	iii) either $(y\downarrow R)/(x\downarrow R) = (y''\downarrow R)/(x'\downarrow R)$	
	or $(x\downarrow R)/(y\downarrow R) = (x'\downarrow R)/(y''\downarrow R)$.	(co-NP)

As P is proper, note that the decidability of $\stackrel{\epsilon}{\Longrightarrow}$ is logspace reducible to the membership problem for left linear cf-grammars, which is in NL, and hence in P. From Lemma 4.7, this procedure is in $\mathrm{NP}^{\mathrm{NP}} = \Sigma_2^p$.
□

Theorem 4.9 *The problem of deciding branching bisimulation for reduced and proper cf-processes is in* Σ_2^p.

Proof.
We decide $u \equiv v$ by applying Corollary 4.5.

Existentially choose a functional relation R in $N \times N^{\leq (n-1)(m-1)+2}$, (NP)
verify that R is basic, (P)
verify that R is self-proving, (Σ_2^p)
verify that $u \downarrow R = v \downarrow R$. (co-NP)

From Lemma 4.6, Proposition 4.8 and Lemma 4.7, this procedure is in Σ_2^p.
□

Proposition 4.10 *There exists a Σ_3^p algorithm for computing a maximal (w.r.t. inclusion) basic self-proving relation.*

Proof.

We extract a maximal basic and self-proving relation by applying Proposition 4.4.

Existentially choose a functional relation R in $N \times N^{\leq (n-1)(m-1)+2}$, (NP)
verify that R is basic, (P)
verify that R is self-proving, (Σ_2^p)
verify that there does not exist co-(
  a functional relation S with $R \subset S \subset N \times N^{\leq (n-1)(m-1)+2}$ such that (NP)
  S is basic, (P)
  S is self-proving. (Σ_2^p))

From Lemma 4.6 and Proposition 4.8, this procedure is in Σ_3^p.
□

LISTE DES DERNIERES PUBLICATIONS INTERNES PARUES A L'IRISA

PI 670 UN RESEAU SYSTOLIQUE INTEGRE POUR LA CORRECTION DE FAUTES DE FRAPPE
Dominique LAVENIER
Juillet 1992, 120 pages.

PI 671 EARLY WARNING OF SLIGHT CHANGES IN SYSTEMS AND PLANTS WITH APPLICATION TO CONDITION BASED MAINTENANCE
Qinghua ZHANG, Michèle BASSEVILLE, Albert BENVENISTE
Juillet 1992, 32 pages.

PI 672 ORDRES REPRESENTABLES PAR DES TRANSLATIONS DE SEGMENTS DANS LE PLAN
Vincent BOUCHITTE, Roland JEGOU, JeanXavier RAMPON
Juillet 1992, 8 pages.

PI 673 AN EXCEPTION HANDLING MECHANISM FOR PARALLEL OBJECT-ORIENTED PROGRAMMING
Valérie ISSARNY
Août 1992, 36 pages.

PI 674 A CALCULUS OF GAMMA PROGRAMS
Chris HANKIN, Daniel LE METAYER, David SANDS
Juillet 1992, 32 pages.

PI 675 EVALUATION DES PERFORMANCES D'UN NOYAU DE SIMULATION REPARTIE
Philippe INGELS, Carlos MAZIERO
Septembre 1992, 36 pages.

PI 676 FONT METRICS
Jacques ANDRE
Septembre 1992, 20 pages.

PI 677 GRIF ET LES INDEX ELECTRONIQUES
Hélène RICHY
Septembre 1992, 40 pages.

PI 678 ETUDE DE QUELQUES ORGANISATIONS D'ANTEMEMOIRES
Nathalie DRACH, André SEZNEC
Octobre 1992, 44 pages.

PI 679 AN ADAPTIVE SPARSE UNSYMMETRIC LINEAR SYSTEM SOLVER
Miloud SADKANE, Roger B. SIDJE
Octobre 1992, 28 pages.

PI 680 BRANCHING BISIMULATION FOR CONTEXT-FREE PROCESSES
Didier CAUCAL, Dung HUYNH, Lu TIAN
Octobre 1992, 36 pages.

ISSN 0249-6399